Vertrauen bei Online-Transaktionen – Vertrauenstypen im Online-Entscheidungsfindungsprozess

DISSERTATION

der Universität St.Gallen,
Hochschule für Wirtschafts-,
Rechts- und Sozialwissenschaften
sowie Internationale Beziehungen (HSG)
zur Erlangung der Würde einer
Doktorin der Wirtschaftswissenschaften

vorgelegt von
Andrea Chandra von Kaenel
von
Greifensee (Zürich) und Reichenbach (Bern)

Genehmigt auf Antrag von
Frau Prof. Dr. Miriam Meckel
und
Herrn Prof. Dr. Urs Gasser

Dissertation Nr. 4190

D-Druck Spescha, St.Gallen 2013

Die Universität St.Gallen, Hochschule für Wirtschafts-, Rechts- und Sozialwissenschaften sowie Internationale Beziehungen (HSG), gestattet hiermit die Drucklegung der vorliegenden Dissertation, ohne damit zu den darin ausgesprochenen Anschauungen Stellung zu nehmen.

St.Gallen, den 17. Mai 2013

Der Rektor:

Prof. Dr. Thomas Bieger

Inhaltsverzeichnis

INHALTSVERZEICHNIS III

DAS DISSERTATIONSPROJEKT IM ÜBERBLICK IX

ABSTRACT XI

ABBILDUNGSVERZEICHNIS XIII

TABELLENVERZEICHNIS XXI

ABKÜRZUNGSVERZEICHNIS XXIII

1 EINFÜHRUNG IN DAS THEMA 1

1.1 Einleitung 1

1.2 Zielsetzung, Forschungsfragen und Relevanz 5

1.2.1 Zielsetzung und Forschungsfragen des Dissertationsvorhabens 5

1.2.2 Wissenschaftliche Relevanz und Forschungslücke 8

1.2.3 Praktische Relevanz 10

1.3 Aufbau der Dissertation 11

1.4 Abgrenzung und Einschränkung der Thematik 16

2 ZUSAMMENHANG ZWISCHEN DATENFREIGABE, PRIVACY UND VERTRAUEN IN DER LITERATUR 21

2.1 Die Ausgangslage: Persönliche Daten sind die neue Währung 22

2.1.1 Die Sozialen Medien führen zu neuen Geschäftsmodellen 22

2.1.1.1 Die Entwicklung in den Sozialen Medien stellt die Gesellschaft vor neue Herausforderungen 22

2.1.1.2 Warum es wichtig ist, sich Gedanken über Geschäftsmodelle zu machen 24

2.1.1.3 Hauptkomponenten, Klassifizierung und Operationalisierung von Online-Geschäftsmodellen 26

2.1.2 Wirtschaftsgut Information bei Online-Transaktionen 31
2.1.2.1 Ohne Daten kein Business 31
2.1.2.2 Daten sind Business 33
2.1.2.3 Die Offenlegung persönlicher Daten im Internet 37
2.1.3 Die Entscheidungsfindung im Internet 41
2.1.3.1 Die Erforschung des Konsumentenverhaltens 41
2.1.3.2 Vom Problemlösungsprozess zum Entscheidungsfindungsprozess 42
2.1.4 Zusammenfassung 47
2.2 Das Problem: Privacybedenken und der Wunsch nach Kontrolle 48
2.2.1 Entstehungsgeschichte und Definition von Privacy 48
2.2.1.1 Der erste Meilenstein: „The Right to Privacy“ 49
2.2.1.2 Literaturübersicht und Diskussion des Konstrukts Privacy 50
2.2.1.3 Die Privacy von Konsumenten und Nutzern 52
2.2.2 Bedeutung von Privacy im Internetzeitalter 54
2.2.2.1 Veränderung von Privacy durch das Internet 55
2.2.2.2 Privacybedenken im Internetkontext 58
2.2.3 Einflussfaktoren auf Privacybedenken und Strategien zum Schutz der Privacy 62
2.2.3.1 Einflussfaktoren auf Privacybedenken 63
2.2.3.2 Nutzerstrategien zum Schutz der Privacy 67
2.2.3.3 Firmeninitiativen zur Reduktion von Privacybedenken 70
2.2.4 Zusammenfassung 74
2.3 Die Lösung: Vertrauen aufbauen 76
2.3.1 Einführung in das Thema Vertrauen und definitorische Abgrenzung 77
2.3.1.1 Definition Vertrauen 77
2.3.1.2 Vertrauensforschung im Internet 80
2.3.1.3 Die Bedeutung von Vertrauen für Anbieter von Online-Geschäftsmodellen 81
2.3.2 Entstehung von Vertrauen 85
2.3.2.1 Einführung in die Einflussfaktoren auf Vertrauen 85

2.3.2.2 Zentrale Vertrauensfaktoren im Online-Bereich 87
2.3.2.3 Literaturüberblick über die zentralen Vertrauensfaktoren 96
2.3.3 Vertrauen als Ergebnis 99
2.3.3.1 Vertrauen als dynamischer Prozess 99
2.3.3.2 Die Absicht, in Zukunft zu vertrauen 101
2.3.4 Zusammenfassung 104

3 FORSCHUNGSMETHODISCHES VORGEHEN 107

3.1 Forschungsmethodische Vorarbeiten 108
3.1.1 Qualitative Befragung von Anbietern und Nutzern von Online-Geschäftsmodellen 108
3.1.2 Fragebogenkonzeption und quantitative Datenerhebung 114
3.1.3 Untersuchungskontext 117
3.1.4 Auswertung der Vertrauensfaktoren und des Vertrauensmasses 119
3.1.5 Zusammenfassung der Vorarbeiten 125

3.2 Hauptuntersuchung 126
3.2.1 Identifikation von Vertrauenstypen 126
3.2.2 Relevante Vertrauensfaktoren pro Vertrauenstyp 137
3.2.3 Vertrauensabsicht pro Vertrauenstyp 139
3.2.4 Zusammenfassung der Hauptuntersuchung 141

4 DISKUSSION DER ERGEBNISSE 143

4.1 Jeder vertraut anders: Interpretation der drei Vertrauenstypen 144
4.1.1 Interpretation Vertrauenstyp 1 145
4.1.1.1 Interpretation Vertrauenstyp 1 aufgrund der Clusterung 145
4.1.1.2 Interpretation Vertrauenstyp 1 anhand demografischer Unterscheidungsmerkmale sowie der Internetnutzung 148
4.1.2 Interpretation Vertrauenstyp 2 157
4.1.2.1 Interpretation Vertrauenstyp 2 aufgrund der Clusterung 157
4.1.2.2 Interpretation Vertrauenstyp 2 anhand demografischer Unterscheidungsmerkmale sowie der Internetnutzung 160
4.1.3 Interpretation Vertrauenstyp 3 166

4.1.3.1 Interpretation Vertrauenstyp 3 aufgrund der Clusterung 166
4.1.3.2 Interpretation Vertrauenstyp 3 anhand demografischer Unterscheidungsmerkmale sowie der Internetnutzung 169
4.1.4 Gegenüberstellung und Benennung der drei Vertrauenstypen 175
4.2 Jeder achtet auf andere Indikatoren: Relevante Vertrauensfaktoren pro Vertrauenstyp 180
4.2.1 Relevante Vertrauensfaktoren für den Skeptiker (Vertrauenstyp 1) 180
4.2.2 Relevante Vertrauensfaktoren für den Praktiker (Vertrauenstyp 2) 188
4.2.3 Relevante Vertrauensfaktoren für den Sozialen (Vertrauenstyp 3) 203
4.3 Jeder reagiert anders: Vertrauensabsichten pro Vertrauenstyp 216
4.3.1 Vertrauensabsichten des Skeptikers (Vertrauenstyp 1) 219
4.3.2 Vertrauensabsichten des Praktikers (Vertrauenstyp 2) 220
4.3.3 Vertrauensabsichten des Sozialen (Vertrauenstyp 3) 221
4.4 Zusammenfassung 223
5 SCHLUSSFOLGERUNG UND AUSBLICK 227
5.1 Schlussfolgerungen für die Vertrauensforschung 227
5.1.1 Theoretische Erkenntnisse 227
5.1.2 Empirische Erkenntnisse 231
5.1.3 Weitere Erkenntnisse aus Theorie und Empirie 233
5.2 Schlussfolgerungen für das Vertrauensmanagement 236
5.2.1 Zentrale Erkenntnisse des Vertrauensmanagements für die Praxis 236
5.2.2 Handlungsempfehlungen für Anbieter von Online-Geschäftsmodellen 243
5.2.2.1 Handlungsempfehlungen für den Skeptiker (Vertrauenstyp 1) 244
5.2.2.2 Handlungsempfehlungen für den Praktiker (Vertrauenstyp 2) 249
5.2.2.3 Handlungsempfehlungen für den Sozialen (Vertrauenstyp 3) 254
5.3 Stärken und Limitationen der vorliegenden Arbeit 260
5.4 Ausblick 263
5.4.1 Bereiche mit weiterem Forschungspotenzial 263
5.4.2 Ein Blick in die Zukunft 267

6 LITERATUR- UND QUELLENVERZEICHNIS 271

7 ANHANG 303

7.1 Anhang zum Literaturteil 303

7.1.1 Übersicht über Geschäftsmodelldefinitionen mit Klassifizierung 303

7.1.2 Definition der elf Kategorien von Geschäftsmodellen nach Timmers (1998; 2000) 306

7.2 Qualitative Befragung der Anbieter 308

7.2.1 Leitfaden der Anbieter-Befragung 308

7.2.2 Übersicht der geführten Interviews mit Anbietern von Online-Geschäftsmodellen 309

7.3 Qualitative Befragung der Nutzer 310

7.3.1 Leitfaden der Nutzer-Befragung 310

7.3.2 Übersicht der geführten Interviews mit Nutzern von Online-Geschäftsmodellen 311

7.4 Quantitative Online-Umfrage 312

7.4.1 Fragebogen der Online-Umfrage 312

7.4.2 Zusammensetzung der Stichprobe der Online-Umfrage (n = 1'549) 318

7.4.3 Finale Item-Liste der Vertrauensfaktoren 319

7.4.4 Faktorladungsmatrix für die Auswertung der Vertrauensfaktoren 321

7.4.5 Rotierte Faktorladungen und Extraktionswerte für die Auswertung der Vertrauensfaktoren 323

7.4.6 Faktorladungsmatrix für die Auswertung des Vertrauensmasses 325

7.4.7 Rotierte Faktorladungen und Extraktionswerte für die Auswertung des Vertrauensmasses 326

7.5 Auswertung der Vertrauenstypen (Forschungsfrage 1) 328

7.5.1 Mögliche zu verwendende Cluster-Algorithmen 328

7.5.2 Zuordnungsübersicht anhand des Ward-Verfahrens (Ausschnitt) 329

7.5.3 Dendrogramm des Ward-Verfahrens 330

7.5.4 Vertrauen in den Anbieter pro Vertrauenstyp in Prozent 331

7.5.5 Vertrauensneigung pro Vertrauenstyp in Prozent 333

7.5.6 Vertrauen in die Institution pro Vertrauenstyp in Prozent 334

7.5.7 Demografie und Internetnutzung pro Vertrauenstyp in Prozent 335

7.5.8 Internetkompetenzen pro Vertrauenstyp in Prozent 340

7.5.9 Gewähltes Online-Geschäftsmodells pro Vertrauenstyp in Prozent 342
7.5.10 Typenunterscheidung anhand der „Keine Antwort"-Rate in Prozent 344

7.6 Auswertung der Vertrauenstypen anhand der Vertrauensfaktoren (Forschungsfrage 2) 345

7.6.1 Items der Vertrauensfaktoren anhand des Mittelwertes pro Vertrauenstyp 345
7.6.2 Items des Faktors Reziprozität pro Vertrauenstyp in Prozent 347
7.6.3 Items des Faktors Marke und Design pro Vertrauenstyp in Prozent 350
7.6.4 Items des Faktors Nutzerkontrolle pro Vertrauenstyp in Prozent 352
7.6.5 Items des Faktors Kundenservice pro Vertrauenstyp in Prozent 354

7.7 Auswertung der Vertrauenstypen anhand des Faktors Vertrauensabsicht (Forschungsfrage 3) 356

7.7.1 Items des Faktors Vertrauensabsicht pro Vertrauenstyp in Prozent 356

7.8 Lebenslauf 357

Das Dissertationsprojekt im Überblick

Anbieter von Online-Geschäftsmodellen stehen vor der Herausforderung, dass Kunden im Internet ein höheres Risiko als in traditionellen Vertriebskanälen wahrnehmen. Bei jeder Transaktion geben Internetnutzer persönliche Daten von sich preis, wobei in den letzten Jahren eine immer stärker werdende Diskrepanz im Umgang mit persönlichen Daten zu beobachten ist. Auf der einen Seite wird viel und freizügig aus dem Privatleben berichtet, andererseits sorgen sich die Nutzer zunehmend, dass sie immer mehr zu gläsernen Kunden werden. Aufbereitete persönliche Nutzerdaten sind der neue Schlüssel zum Erfolg von Online-Geschäftsmodellen, doch das Streben der Anbieter nach möglichst vielen privaten Nutzerdaten löst bei den Nutzern Privacybedenken aus, die sie daran hindern, ihre Transaktionen online zu tätigen. Privacybedenken gelten als zentrale Hürde beim Wachstum von Online-Geschäftsmodellen, denn die Bereitschaft der Nutzer, einem Transaktionspartner persönliche Daten zur Verfügung zu stellen, ist Voraussetzung für jede Art von Online-Transaktion. Das Vertrauen der Nutzer ist zu einer elementaren Grundbedingung geworden und spielt eine entscheidende Rolle für das Zustandekommen von Transaktionen im Internet. Die Bereitschaft zu vertrauen variiert jedoch von Mensch zu Mensch, denn Individuen bauen unterschiedlich schnell und aus verschiedenen Beweggründen heraus Vertrauen zu anderen Menschen oder Institutionen auf.

Diese Dissertation hat zum Ziel, die Bedeutung des Nutzervertrauens für die Durchführung von Online-Transaktionen zu erforschen, um Handlungsempfehlungen für Anbieter von Online-Geschäftsmodellen generieren zu können. Insbesondere wird erforscht, welche Massnahmen geeignet sind, Nutzervertrauen aufzubauen und aufrechtzuerhalten. Dafür wird der Literaturzusammenhang zwischen Datenfreigabe, Privacy und Vertrauen im Internet beleuchtet. Das übergeordnete Forschungsziel der Dissertation ist, Personengruppen im Internet nach ihren Vertrauenseigenschaften in Typen zu unterscheiden. Im Rahmen dieser Studie wurden 1’549 Nutzer von Online-Geschäftsmodellen mittels quantitativem Fragebogen über ihr Internetverhalten befragt. Durch eine Clusteranalyse wurden drei unterschiedliche Vertrauenstypen identifiziert und mittels Faktorenanalysen und Mittelwertvergleichen wurden die relevanten Vertrauensfaktoren und Vertrauensabsichten den Vertrauenstypen zugeordnet.

Die identifizierten Vertrauenstypen sind „der Skeptiker“, „der Praktiker“ und „der Soziale“. Diese drei Typen achten während einer Transaktion im Internet auf unterschiedliche Vertrauensfaktoren, sie lassen sich jedoch nicht aufgrund ihrer zukünftigen Vertrauensabsichten unterscheiden. Die Resultate der Arbeit verdeutlichen einerseits die Wichtigkeit von Vertrauen bei Online-Transaktionen und andererseits die Schwierigkeit für Anbieter von Online-Geschäftsmodellen, zielgruppengerecht Vertrauen zu generieren und zu erhalten. Online-Vertrauensmanagement ist der kritische Erfolgsfaktor für die Unternehmenskommunikation und muss als ganzheitliche und langfristige Aufgabe gesehen werden.

Abstract

Providers of online applications face the challenge of an increased perception of risk on the Internet, compared to traditional (sales) channels. In every interaction, Internet users provide personal information whereas in the last years, an increased discrepancy can be observed in the handling of their personal data. On the one hand, users report private information freely and in an almost exhibitionist manner, while, on the other, they worry more and more about becoming a transparent Internet consumer. The management of personal user data is key to future success for online business models, while the requirement for further data collection leads to privacy concerns among users, preventing them from entering online transactions. Privacy concerns hence represent a central obstacle for growth in business models, as the users' willingness to provide personal data is a prerequisite for online transactions. Users' trust has been established as a precondition to online business and thus plays an important role for the accomplishment of online transactions. The willingness to trust varies from person to person because individuals build trust in other people, or towards institutions, at different paces and on the basis of different reasons.

The goal of this dissertation is to examine the relevance of users' trust during online transactions, in order to generate specific recommendations for online applications providers. The intention is to explore which steps need to be taken to generate and maintain users' trust. Therefore, the dissertation scrutinizes data sharing, privacy and trust in the Internet. The main research objective of this dissertation is to observe the disposition to trust of different groups of people on the basis of trust typologies and employing a process oriented framework. As part of this study, in a quantitative survey 1'549 Internet users were questioned about their online behavior. The application of a cluster analysis led to the identification of three different trust types. The relevant trust factors and trusting intentions were attributed to the trust types through factor analyses and comparisons of means.

The identified trust types are "the Skeptic", "the Practitioner" and "the Social". Those three types rely on different trust factors during an Internet transaction; however, they cannot be clearly distinguished when it comes to their trusting intentions. The results highlight the importance of trust during online transactions. Providers of online applications face the challenge of building and maintaining trust, specific to

their target group. Online trust management is the crucial success factor for corporate communications and must be seen as an integrated and long-term activity.

Abbildungsverzeichnis

Abbildung 1: Übergeordnetes Forschungsziel und Forschungsfragen der Dissertation (eigene Darstellung) 8

Abbildung 2: Struktur der Dissertation (eigene Darstellung) 12

Abbildung 3: Grundlegende Konzepte der Literaturrecherche (eigene Darstellung) 21

Abbildung 4: Die Hauptkomponenten von Geschäftsmodellen (Osterwalder & Pigneur, 2010; Timmers, 1998; Scheer et al., 2003) 26

Abbildung 5: Klassifikation von Geschäftsmodellen nach Timmers (1998; 2000) 29

Abbildung 6: Operationalisierung von Online-Geschäftsmodellen (eigene Darstellung) 30

Abbildung 7: Wo wir was über uns enthüllen (eigene Darstellung) 31

Abbildung 8: Anbieter fordern zur Offenlegung privater Daten auf, am Beispiel von Yammer, StudiVZ, Xing und Netlog (eigene Darstellung) 32

Abbildung 9: Preisliste persönlicher Daten von RapLeaf (Soltani, 2011) 34

Abbildung 10: Einflussfaktoren auf die Offenlegung persönlicher Daten (eigene Darstellung) 37

Abbildung 11: Vom Problemlösungs- zum Entscheidungsfindungsprozess (Dewey, 1910; Engel et al., 1968; 1978; 1986) 43

Abbildung 12: Der Online-Entscheidungsfindungsprozess (eigene Darstellung in Anlehnung an Darley et al., 2010) 45

Abbildung 13: Privacystufen (eigene Darstellung in Anlehnung an Goodwin, 1991) 53

Abbildung 14: Zentrale Privacybedenken (eigene Darstellung in Anlehnung an Nissenbaum, 2009) 59

Abbildung 15: Einflussfaktoren auf Privacybedenken (Sheehan & Hoy, 2000; Phelps et al., 2000; Lanier & Saini, 2008) 63

Abbildung 16: Sensibilität von persönlichen Daten (eigene Darstellung in Anlehnung an Nokia Siemens Networks, 2009) 65

Abbildung 17: Konfrontative Nutzerstrategien zum Schutz der Privacy (eigene Darstellung) 68

Abbildung 18: Unternehmen können Privacybedenken reduzieren oder Vertrauen aufbauen (eigene Darstellung) 71

Abbildung 19: Firmeninitiativen zur Reduktion von Privacybedenken der Nutzer (FTC, 2000; Milne & Boza, 1999; Culnan & Armstrong, 1999) 72

Abbildung 20: Zusammenhang von Privacybedenken, Nutzerstrategien und Firmeninitiativen (eigene Darstellung) 75

Abbildung 21: Vertrauenskomponenten (eigene Darstellung) 77

Abbildung 22: Kernelemente von Vertrauen (eigene Darstellung) 78

Abbildung 23: Web Trust Model (eigene Darstellung in Anlehnung an McKnight et al., 1998; 2002a) 82

Abbildung 24: Relevante Vertrauensfaktoren (eigene Darstellung) 87

Abbildung 25: Beispiele von Vertrauenszertifikaten (eigene Darstellung) 91

Abbildung 26: Drei Phasen von Vertrauen (eigene Darstellung in Anlehnung an Rousseau et al., 1998) 99

Abbildung 27: Online-Entscheidungsfindungsprozess und die Vertrauensphasen (eigene Darstellung) 101

Abbildung 28: Vertrauensabsicht (eigene Darstellung in Anlehnung an McKnight et al., 2002a) 102

Abbildung 29: Zusammenhang zwischen Vertrauen, dem Entscheidungsfindungsprozess und den Forschungsfragen (eigene Darstellung) 104

Abbildung 30: Forschungsmethodisches Vorgehen (eigene Darstellung) 107

Abbildung 31: Interviewte Anbieter von Online-Geschäftsmodellen (eigene Darstellung) 109

Abbildung 32: Interviewte Nutzer von Online-Geschäftsmodellen (eigene Darstellung) 111

Abbildung 33: Relevante Vertrauensfaktoren (Hoffmann, Meckel & von Kaenel, 2010b) 112

Abbildung 34: Konzeption des Fragebogens (eigene Darstellung) 115

Abbildung 35: Ablaufschritte der Faktorenanalyse (eigene Darstellung in Anlehnung an Backhaus et al., 2011) 120

Abbildung 36: Zusammenfassung der Vertrauensfaktoren und des Vertrauensmasses (eigene Darstellung) 125

Abbildung 37: Ablaufschritte der Clusteranalyse (eigene Darstellung in Anlehnung an Backhaus et al., 2011) 127

Abbildung 38: Elbow-Kriterium zur Bestimmung der optimalen Clusterzahl (eigene Darstellung) 130

Abbildung 39: Vertrauenstypen anhand des relativen Mittelwertes (Interpretation: negative Werte tendieren zu „trifft zu“, positive Werte zu „trifft nicht zu“) 131

Abbildung 40: Ablaufschritte der Diskriminanzanalyse (eigene Darstellung in Anlehnung an Backhaus et al., 2011) 132

Abbildung 41: Grafische Darstellung der Vertrauenstypen im Diskriminanzraum (SPSS Output) 136

Abbildung 42: Zusammenfassung der relevanten Vertrauensfaktoren pro Vertrauenstyp (Interpretation: negative Werte tendieren zu „trifft zu“, positive Werte zu „trifft nicht zu“) 139

Abbildung 43: Zusammenfassung der forschungsmethodischen Ergebnisse (eigene Darstellung) 141

Abbildung 44: Übersicht über das Kapitel 4 „Diskussion der Ergebnisse“ (eigene Darstellung) 143

Abbildung 45: Analyse Vertrauenstyp 1 anhand des Mittelwertes Ø (Interpretation: negative Werte tendieren zu „trifft zu“, positive Werte zu „trifft nicht zu“) 145

Abbildung 46: Typenunterscheidung anhand des Alters in Prozent (V_136) 150

Abbildung 47: Typenunterscheidung anhand des gewählten Online-Geschäftsmodells in Prozent (V_177) 152

Abbildung 48: Typenunterscheidung anhand der Internetkompetenzen in Prozent bei „trifft zu“ und „trifft eher zu“ 156

Abbildung 49: Analyse Vertrauenstyp 2 anhand des Mittelwertes Ø (Interpretation: negative Werte tendieren zu „trifft zu“, positive Werte zu „trifft nicht zu“) 157

Abbildung 50: Analyse Vertrauenstyp 3 anhand des Mittelwertes Ø (Interpretation: negative Werte tendieren zu „trifft zu“, positive Werte zu „trifft nicht zu“) 166

Abbildung 51: Der Skeptiker (eigene Darstellung) 177

Abbildung 52: Der Praktiker (eigene Darstellung)..... 178

Abbildung 53: Der Soziale (eigene Darstellung) 179

Abbildung 54: Relevante Vertrauensfaktoren für den Skeptiker (Vertrauenstyp 1) (eigene Darstellung) 181

Abbildung 55: Besonders auffällige Antwortstrukturen des Skeptikers (eigene Darstellung)..... 182

Abbildung 56: Nutzen und Verpflichtungen bei Blacksocks (Blacksocks, 2012)..... 183

Abbildung 57: Wahlmöglichkeit zwischen Registrierung oder Direktbestellung bei Posterjack (Posterjack, 2012) 185

Abbildung 58: Registrierung mit wenigen Pflichtfeldern bei Cineman (Cineman, 2012)..... 186

Abbildung 59: Kontaktmöglichkeiten bei Zalando (Zalando, 2012)..... 187

Abbildung 60: Relevante Vertrauensfaktoren für den Praktiker (Vertrauenstyp 2) (eigene Darstellung) 188

Abbildung 61: Mittelwerte der Items des Faktors Reziprozität des Praktikers (Interpretation: 1 „trifft zu“; 5 „trifft nicht zu“) 189

Abbildung 62: Visualisierung zur Sicherheit und Datenschutz bei Mycare (Mycare, 2012) 190

Abbildung 63: Ausführliche Informationen bei Google (Google, 2012) 191

Abbildung 64: Mittelwerte der Items des Faktors Marke und Design des Praktikers (Interpretation: 1 „trifft zu“; 5 „trifft nicht zu“) 192

Abbildung 65: Diskussion über Crowdfunding auf DRS 2 (DRS 2, 2012; Wemakeit, 2012; 100Days, 2012) 194

Abbildung 66: Terminfindung leicht gemacht bei Doodle (Doodle, 2012) 195

Abbildung 67: Mittelwerte der Items des Faktors Kundenservice des Praktikers (Interpretation: 1 „trifft zu“, 5 „trifft nicht zu“) 196

Abbildung 68: Kundenintegration bei Starbucks (Starbucks, 2012) 198

Abbildung 69: Kundenservice über Twitter bei der Telekom (Telekom, 2012) 199

Abbildung 70: Mittelwerte der Items des Faktors Nutzerkontrolle des Praktikers (Interpretation: 1 „trifft zu“, 5 „trifft nicht zu“) 200

Abbildung 71: Kontrolle über die eigenen Daten bei Xing (Xing, 2012) 201

Abbildung 72: Auf den Praktiker zugeschnittene Registrierung bei eDarling (eDarling, 2012) 202

Abbildung 73: Relevante Vertrauensfaktoren für den Sozialen (Vertrauenstyp 3) (eigene Darstellung) 203

Abbildung 74: Mittelwerte der Items des Faktors Marke und Design des Sozialen (Interpretation: 1 „trifft zu“, 5 „trifft nicht zu“) 204

Abbildung 75: Verweis auf die Marktmacht bei eBay (eBay, 2012) 205

Abbildung 76: Verweis auf die Anzahl Nutzer des Studienwahl-Navigators (HAW-Hamburg, 2012) 206

Abbildung 77: Schlichtes Design und schweizerdeutscher Slogan bei Zalando (Zalando, 2012) 207

Abbildung 78: Mittelwerte der Items des Faktors Kundenservice des Sozialen (Interpretation: 1 „trifft zu“, 5 „trifft nicht zu“) 209

Abbildung 79: Avatar als Kundensupport beim Salzlandkreis (Salzlandkreis, 2012) 210

Abbildung 80: Live Chat Support nach den Bürozeiten (Eat, 2012) 211

Abbildung 81: Animation zur Nutzerpartizipation bei Migipedia (Migipedia, 2012) 212

Abbildung 82: Mittelwerte der Items des Faktors Reziprozität des Sozialen (Interpretation: 1 „trifft zu“, 5 „trifft nicht zu“) 213

Abbildung 83: Verpflichtungen bei DaWanda (DaWanda, 2012) 214

Abbildung 84: Erfolgsgeschichten bei Parship (Parship, 2012) 215

Abbildung 85: Mittelwertvergleich der Vertrauenstypen anhand des Faktors Vertrauensabsicht (Interpretation: negative Werte tendieren zu „trifft zu“, positive Werte zu „trifft nicht zu“) 216

Abbildung 86: Drei Vertrauenstypen auf einen Blick (eigene Darstellung) 223

Abbildung 87: Zusammenfassung der Ergebnisse (eigene Darstellung) 225

Abbildung 88: Zusammenfassung der theoretischen Erkenntnisse (eigene Darstellung) 230

Abbildung 89: Zusammenfassung der empirischen Erkenntnisse (eigene Darstellung) 232

Abbildung 90: Zentrale Erkenntnisse des Vertrauensmanagements für die Praxis (eigene Darstellung) 236

Abbildung 91: Anzahl der Wörter der Privacy-Statements bei Facebook (eigene Darstellung in Anlehnung an Gates, 2010) 240

Abbildung 92: Handlungsempfehlungen für den Skeptiker (eigene Darstellung) ... 244

Abbildung 93: Handlungsempfehlungen für den Praktiker (eigene Darstellung) ... 249

Abbildung 94: Handlungsempfehlungen für den Sozialen (eigene Darstellung) 255

Abbildung 95: Überblick über mögliche Cluster-Algorithmen (eigene Darstellung in Anlehnung an Backhaus et al., 2011) 328

Abbildung 96: Typenunterscheidung anhand des konkreten Online-Anbieters in Prozent (V_178) 343

Tabellenverzeichnis

Tabelle 1: Literaturüberblick über die zentralen Vertrauensfaktoren 97

Tabelle 2: Kaiser-Meyer-Olkin-Kriterium und Barlett-Test für die Auswertung der Vertrauensfaktoren 121

Tabelle 3: Explorative Faktorenanalyse für die Auswertung der Vertrauensfaktoren 121

Tabelle 4: Absolute Mittelwerte Ø der Vertrauensfaktoren (Interpretation :1 „trifft zu“, 5 „trifft nicht zu“) 121

Tabelle 5: Kaiser-Meyer-Olkin-Kriterium und Barlett-Test für die Messung des Vertrauensmasses 123

Tabelle 6: Explorative Faktorenanalyse für die Messung des Vertrauensmasses 124

Tabelle 7: Absolute Mittelwerte Ø des Vertrauensmasses (Interpretation: 1 „trifft zu“, 5 „trifft nicht zu“) 124

Tabelle 8: Analyse der Vertrauenstypen anhand des relativen Mittelwertes (Interpretation: negative Werte tendieren zu „trifft zu“, positive Werte zu „trifft nicht zu“) 130

Tabelle 9: Eigenwert zur Prüfung der Diskriminanzfunktionen (* Die zwei ersten kanonischen Diskriminanzfunktionen wurden in der Analyse verwendet.) 133

Tabelle 10: Wilks’ Lambda zur Prüfung der Diskriminanzfunktionen 134

Tabelle 11: Prüfung der Merkmalsvariablen 134

Tabelle 12: Standardisierte Diskriminanzkoeffizienten 134

Tabelle 13: Fishers lineare Klassifizierungsfunktion 135

Tabelle 14: Klassifizierungsergebnisse (die Trefferquote beträgt 82.3 %) 136

Tabelle 15: Kruskal-Wallis-Test der Vertrauensfaktoren (Kruskal Wallis Test / Grouping Variable: Ward-Method CLU3_1) 137

Tabelle 16: Effektive Mittelwertabweichungen der Vertrauensfaktoren pro Vertrauenstyp (Interpretation: negative Werte tendieren zu „stark beachtet“, positive Werte zu „nicht beachtet“) 138

Tabelle 17: Kruskal-Wallis-Test der Vertrauensabsicht (Kruskal Wallis Test / Grouping Variable: Ward-Method CLU3_1 140

Tabelle 18: Mittelwertvergleich des Faktors Vertrauensabsicht pro Vertrauenstyp (Interpretation: negative Werte tendieren zu „trifft zu“, positive Werte zu „trifft nicht zu“) 140

Tabelle 19: Signifikanzen der Demografie und der Internetnutzung 149

Tabelle 20: Gegenüberstellung der drei Vertrauenstypen 175

Abkürzungsverzeichnis

€	Euro
∑	Summe / Total
A	Anbieter
AGB	Allgemeine Geschäftsbedingungen
B2B	Business-to-Business
B2C	Business-to-Consumer/Customer
bspw.	beispielsweise
bzw.	beziehungsweise
ca.	circa
CEO	Chief Executive Officer
CFIP	Concern for Information Privacy
CMO	Chief Marketing Officer
CRM	Customer Relationship Management
d. h.	das heisst
Dr.	Doktor
e. g.	exempli gratia / for example
EKB-Modell	Engel-Kollat-Blackwell-Modell
et al.	und weitere
f.	folgende Seite
FAQ	Frequently Asked Questions
ff.	fortfolgende Seiten
FTC	Federal Trade Commission
Hrsg.	Herausgeber
ICA	International Communication Association
ICT	Information & Communication Technology

IDC	International Data Corporation
IKT	Informations- & Kommunikationstechnologie
Mio.	Million/Millionen
N	Nutzer
NV	Normalverteilung
Ø	Mittelwert
o. S.	ohne Seitenangabe
PR	Public Relations
Prof.	Professor/Professorin
r	Korrelationskoeffizient
RFID	Radio-frequency identification
S.	Seite
SEO	Search Engine Optimization
StBA	Statistisches Bundesamt Deutschland
TAM	Technology Acceptance Model
usw.	und so weiter
vs.	versus
www	World Wide Web
z. B.	zum Beispiel
zit.	zitiert

1 Einführung in das Thema

Dieses Kapitel dient der Einführung in das Forschungsgebiet Vertrauensmanagement bei Online-Transaktionen. Im Kapitel 1.1 wird zuerst auf die Problematik der Unsicherheit der Nutzer bei Online-Transaktionen eingegangen und es werden die Kernpunkte der aktuellen Debatte des Forschungsthemas aufgezeigt. Das folgende Kapitel 1.2 diskutiert die Zielsetzung und skizziert die praktische und wissenschaftliche Relevanz des Dissertationsvorhabens. Die zugrunde liegenden Forschungsfragen werden abgeleitet und das Forschungsthema abgegrenzt. Im Kapitel 1.3 wird der Aufbau der Dissertation vorgestellt und abschliessend wird im Kapitel 1.4 auf die Einschränkung der Thematik eingegangen.

1.1 Einleitung

Seit Ende der 90er-Jahre herrscht rund um das Internet regelrechte Aufbruchsstimmung (Hoffman, Novak & Peralta, 1999a). Der Crash der New Economy durch das Platzen der Dotcom-Blase im Jahre 2000 versetzte dem Wachstum zwar einen Rückschlag, vermochte das stetige Voranschreiten jedoch nicht aufzuhalten (Schmidt, 2011). In Deutschland sind 74.7 % der Gesamtbevölkerung online und der Onliner-Anteil wächst jährlich um 2.7 % ((N)Onliner Atlas, 2012). Der Umsatz der E-Commerce-Branche in Deutschland liegt im Jahr 2011 erstmals bei mehr als 20 Milliarden Euro, dies entspricht einem Wachstum von 18.5 % gegenüber dem Vorjahr (Wilhelm, 2012). Durch das Internet entstehen stetig neue, innovative Geschäftsmodelle und Tausende Applikationen-Anbieter treten auf den Markt. Nutzer[1] treffen auf diese Anbieter in einem neuen Marktumfeld, in welchem die Rahmenbedingungen wie zum Beispiel die Gesetzgebung, ethische Standards oder die Technik nicht gefestigt sind und sich stetig weiterentwickeln. Durch die Verbreitung und die Ökonomisierung des Internets verändert sich nicht nur die Produktion und Distribution von Gütern und Dienstleistungen, sondern auch die Art und Weise, wie private,

[1] In dieser Arbeit wird abwechslungsweise der Begriff Nutzer und Kunde verwendet. Um das Lesen nicht zu erschweren, werden nicht jedes Mal der Nutzer und der Kunde erwähnt. Gemeint sind aber immer beide.

nicht-öffentliche und öffentliche Daten im Internet gehandhabt und wahrgenommen werden (Dürscheid, 2007).

Ein Vorteil des Internets sind massgeschneiderte Lösungen sowie personalisierte Produkte und Dienstleistungen. Im Internet ist es ohne viel technischen Aufwand möglich, aufgrund von vergangenem Nutzerverhalten auf die Zukunft zu schliessen, und in diesem Bereich entstehen kontinuierlich neue Angebote (Montgomery & Smith, 2009; Joinson, Woodley & Reips, 2007). Bei jeder Interaktion im Netz, wenn wir eine Transaktion tätigen oder wenn wir im Internet surfen, geben wir persönliche Daten von uns preis (Metzler, 2012). Diese Spuren im Internet lassen sich wie die Steine eines Mosaiks zu einem Gesamtbild unserer selbst zusammensetzen (Schuppisser, 2012). Für Anbieter von Online-Geschäftsmodellen wird es immer wichtiger, eine möglichst stabile und nachhaltige Nutzerbeziehung aufzubauen und gleichzeitig möglichst viele Daten über den Nutzer zu sammeln, um massgeschneiderte Produkte anbieten zu können. Aufbereitete persönliche Daten sind der neue Schlüssel zum Erfolg und somit die neue Währung im Internet. Der Autor Leonhard (2011) bezeichnet Daten als das neue Öl und führt weiter aus, dass Data-Mining-Unternehmen in Zukunft mehr Macht haben werden als Firmen wie Shell, Exxon und Mobil heute zusammen besitzen. Bereits heute wächst das Datenvolumen im Netz in horrendem Tempo, es verdoppelt sich alle zwei Jahre (Schuppisser, 2012). Der Schweizer Datenschützer Hanspeter Thür gibt in diesem Zusammenhang zu bedenken, dass die Verknüpfungsmöglichkeiten und damit die Qualität des Data Mining immer besser werden und dass sich dadurch ein gewisses Konfliktpotenzial zwischen Datenschutz und Marketing ergibt (Hermes & Thür, 2011). Roland Meyer (2011), CMO einer Direktmarketingfirma, bezeichnet die Datenschutzthematik sogar als *die* Herausforderung unserer Zeit. Der Hunger nach möglichst vielen privaten Nutzerdaten gewisser Firmen löst bei den Nutzern Privacybedenken aus, die sie daran hindern, ihre Transaktionen online zu tätigen.

In den letzten Jahren ist unter den Internetnutzern eine immer stärker werdende Diskrepanz im Umgang mit ihren persönlichen Daten zu beobachten. Auf der einen Seite wird auf sozialen Netzwerkseiten in grossen Mengen freizügig aus dem Privatleben berichtet, andererseits sorgen sich die Nutzer um die Handhabung ihrer persönlichen Daten durch die Anbieter. Dass Nutzer ihren Spass im freizügigen Austausch suchen und gleichzeitig Privatheit reklamieren können, nennt der Journalist Güntner (2010) eine Illusion. Da wir immer mehr Zeit unseres Lebens im Internet verbringen, beruflich wie auch privat, steigt der Bedarf, die Weitergabe und Vertei-

lung von Information vor dem Zugriff Dritter zu schützen oder diese zu kontrollieren – die faktische Kontrolle des Individuums über die eigenen Daten wird jedoch immer geringer (Drüeke & Weber, 2007). Dies führt dazu, dass Nutzer in Zukunft vermehrt darauf achten werden, wem sie welche Daten wo zur Verfügung stellen.

Diese Bedenken werden als zentrale Hürde beim Wachstum von Online-Geschäftsmodellen gesehen, denn die Bereitschaft der Nutzer, einem Transaktionspartner persönliche Daten zur Verfügung zu stellen, ist Grundvoraussetzung für jede Art von Online-Transaktion (Culnan & Armstrong, 1999; Milne & Boza, 1999; Eastlick, Lotz & Warrington, 2006). Der Wirtschaftswissenschaftler Kotler formuliert dieses Grundproblem folgendermassen: "We are becoming aware that business is gathering data about us every time we use the Internet. Those with low trust are using the Internet less. Businesses with a good reputation for integrity will have more customers trusting them." (Kotler, E-Mail, 16.05.2011). Auf der einen Seite stehen die Bedenken der Nutzer, persönliche Daten zur Verfügung zu stellen, auf der andere Seite versuchen Anbieter von Online-Geschäftsmodellen, die Offenlegung von persönlichen Daten unter den Nutzern zu fördern, um möglichst viele Informationen über ihre Kunden zu generieren (Taraszow, Aristodemou, Shitta, Laouris & Arsoy, 2010).

Unternehmen sind nicht einfach nur Wirtschaftsakteure, sondern sie werden auch aufgrund ihrer sozialen und umweltbezogenen Aufgaben von der Öffentlichkeit gemessen und beurteilt (Wiedemann, 1994). Schon immer mussten sich Unternehmen mit öffentlichen Debatten und Kritik auseinandersetzen, das Web 2.0 aber hat die potenzielle Gefahr für einen Reputationsschaden, zum Beispiel durch einen Hackerangriff oder einen Datenschutzskandal, deutlich erhöht (Burns, 2007). Leider ist es so, dass sich unter den vielen neuen Online-Anbietern und den Abertausenden von Nutzern auch schwarze Schafe befinden (Rosenbach & Schmundt, 2011). In den letzten Monaten wurden immer wieder skandalöse Datenschutzverletzungen aufgedeckt, welche das Nutzervertrauen in seinen Grundfesten erschüttert haben. Zum Beispiel wurden persönliche Profile von Jugendlichen aus dem sozialen Netzwerk SchülerVZ geklaut (Seidler, 2009) oder Kreditkarteninformationen und Passwörter bei Sony Playstation veröffentlicht (Kremp, 2011). Der Grosskonzern Apple ortete seine Kunden sogar über Monate metergenau über ihr Mobiltelefon und wertete diese Daten ohne das Wissen der Betroffenen aus (Schmundt, 2011).

Die Kommunikationsgesellschaft ist momentan im Begriff, sich vom Informationszeitalter zu lösen, um sich ins Datenzeitalter zu klicken (Schuppisser, 2012). Ant-

worten auf Fragen in Bezug auf die Sicherheit und Privacy im Online-Bereich werden für Internetnutzer, Behörden und Unternehmen immer zentraler. Es kann nicht davon ausgegangen werden, dass Internetnutzer Anbietern von Online-Geschäftsmodellen stets bereitwillig Vertrauen entgegenbringen (McKnight, Choudhury & Kacmar, 2002a; Urban, Amyx & Lorenzon, 2009). Vertrauen wird in dieser Arbeit als die Bereitschaft der Nutzer verstanden, einem Transaktionspartner persönliche Daten online zur Verfügung zu stellen. Das Vertrauen der Nutzer ist einer der bedeutendsten Erfolgsfaktoren internetbasierter Geschäftsmodelle (Cheskin, 1999; Gefen & Straub, 2003; Luo, 2002; Tan & Thoen, 2002). Im Internet können Nutzer schnell zwischen unterschiedlichsten Anbietern von Online-Geschäftsmodellen auswählen. "Competing businesses are only a mouse click away." (Anderson & Srinivasan, 2003, S. 124). Nutzer müssen sich auf der Seite wohl fühlen und dem Anbieter vertrauen, ansonsten sind sie mit einem Klick beim Konkurrenten.

Vertrauen entsteht in der Regel durch länger andauernde Interaktionen, das heisst kontinuierlich (Hart & Saunders, 1997). Solche fortwährenden Interaktionen sind im Internetkontext indes nur selten anzutreffen. Dies hat zur Konsequenz, dass die Transaktionspartner oft nur über wenige Informationen in Bezug auf die Vertrauenswürdigkeit der anderen Partei verfügen (Gefen, 2000). Somit müssen andere Wege gefunden werden, um Vertrauen im Internetkontext zu erzeugen. Eine weitere Herausforderung sind die Nutzer selbst: Jeder Mensch vertraut anderen Menschen, einer Organisationen oder Technologien individuell anders. Jeder Mensch vertraut unterschiedlich schnell und unterschiedlich intensiv – wenn überhaupt. Ausserdem weisen Internetnutzer sehr unterschiedliche Internetkompetenzen auf und haben eine unterschiedliche Bereitschaft, persönliche Daten zur Verfügung zu stellen (Chelappa & Sin, 2005; Eastlick et al., 2006). Demnach achten auch nicht alle Internetznutzer auf dieselben Vertrauensfaktoren.

Da die Bereitstellung persönlicher Daten im Internet immer wichtiger wird und gleichzeitig die Bedenken der Nutzer zunehmen, wird es notwendig, das Vertrauensmanagement der Anbieter auf eine breitere Grundlage zu stellen. Wie diese Dissertation diesen Herausforderungen entgegenwirken möchte, ist Thema des nächsten Kapitels.

1.2 Zielsetzung, Forschungsfragen und Relevanz

In diesem Kapitel werden die Zielsetzung der Dissertation und die zu beantwortenden Forschungsfragen (Kapitel 1.2.1) sowie die wissenschaftliche (Kapitel 1.2.2) und praktische Relevanz (Kapitel 1.2.3) des Forschungsvorhabens näher erläutert.

1.2.1 Zielsetzung und Forschungsfragen des Dissertationsvorhabens

Trotz massiver Zunahme von Online-Transaktionen hemmen immer noch zahlreiche wahrgenommene Risiken eine breitere Nutzung von Internetdiensten. Bedenken bezüglich der Identität des Handelspartners, finanzielle Risiken oder Bedenken bezüglich der Handhabung der privaten Daten (Bhatnagar, Misra & Rao, 2000; Phelps, D'Souza & Nowak, 2001; Schoenbachler & Gordon, 2002) sind nur eine Auswahl der Nutzerbedenken. Hinzu kommt unter Umständen das Misstrauen gegenüber dem Medium Internet im Allgemeinen (McKnight, Cummings & Chervany, 1998). Die enorme Bedeutung der Bereitstellung persönlicher Daten bei gleichzeitig steigender Gefährdung der Vertrauenswürdigkeit und Reputation von Unternehmen angesichts einer kritischen Medienöffentlichkeit (Lyczek & Meckel, 2008) machen es notwendig, das Vertrauensmanagement von Online-Anbietern auf eine breitere Grundlage zu stellen (Hoffmann, Meckel & von Kaenel, 2010a). Es fehlen jedoch praktische sowie theoretische Erkenntnisse darüber, wie Vertrauen im Online-Kontext erzeugt werden kann und, daraus abgeleitet, wie Anbieter von Online-Geschäftsmodellen diesen Herausforderungen begegnen und die resultierenden Chancen nutzen können.

Vertrauensmanagement ist keine statische Aufgabe, sondern muss in einem dynamischen Rahmen betrachtet werden. Vertrauenseinstellungen ändern sich aufgrund von Interaktionserfahrungen, zusätzlichen Informationen oder weichen Faktoren wie zum Beispiel der Gestaltung einer Homepage. Während einer Online-Transaktion sollten deshalb mehrere unterschiedliche Phasen des Vertrauens differenziert werden (McKnight et al., 2002a; Yoon, 2002; Wang, Beatty & Fox, 2004). Um dem Prozesscharakter der Vertrauensbildung Rechnung zu tragen, wird dieser Arbeit der Entscheidungsfindungsprozess von Engel, Kollat und Blackwell (1978) zugrunde gelegt.

Ziel des vorliegenden Dissertationsprojekts ist es, sowohl das Wirtschaftsgut „persönliche Daten" im Internet, die Geschäftsmodelle als auch den Entscheidungsfin-

dungsprozess des Nutzers im Internet zu beleuchten und einen vertieften Einblick in die Wechselwirkungen zwischen persönlichen Daten, Privacybedenken und Vertrauen zu gewinnen. In dieser Dissertation wird aufgezeigt, dass Vertrauen eine entscheidende Rolle für das Zustandekommen von Transaktionen im Internet zukommt.

Um herausarbeiten zu können, weshalb Menschen im Internet ihre persönlichen Daten zur Verfügung stellen, wann sie Menschen und/oder Institutionen vertrauen, weshalb sie unterschiedlich vertrauen und auf welche Indikatoren sie achten, müssen folgende Fragen geklärt werden: Gehen Menschen im Internet sorgloser mit ihren privaten Daten um als in Offline-Transaktionen? Was ist Privacy? Was zeichnet Privacy im Internet aus? Welche Daten werden als privat erachtet? Besteht ein Bewusstsein für Privacy im Internet? Woher nehmen Nutzer das Vertrauen, dass ihre Daten nicht missbraucht werden? Was ist Vertrauen? Können Nutzer in gewisse Vertrauenstypen eingeteilt werden? Wie kann Vertrauen im digitalen Kontext generiert werden? Wie wird die Bedeutung des Nutzervertrauens eingeschätzt? Welche Faktoren müssen gegeben sein, damit der Sprung von der Angst hin zur Datenfreigabe stattfindet? Spielen „weiche" Faktoren, wie z. B. das Design, bei der Generierung von Vertrauen eine Rolle? Wie äussert sich Vertrauen im Internet? Inwiefern hat die Kommunikation einer Organisation Einfluss auf das Vertrauen der Nutzer? Wie kann eine geeignete Kommunikationsstrategie angesichts der Zielgruppenwahrnehmung aussehen?

Um diese Fragen beantworten zu können, ist es das übergeordnete Forschungsziel der Dissertation, Personengruppen im Internet nach ihren Vertrauenseigenschaften in Typen zu unterscheiden. Damit dieses übergeordnete Forschungsziel erreicht werden kann, stehen folgende drei Hauptfragestellungen im Mittelpunkt dieser Arbeit:

Forschungsfrage 1:

Existieren bei Internetnutzern unterschiedliche Vertrauenstypen?

Jeder Mensch fasst unterschiedlich schnell und aus anderen Beweggründen heraus Vertrauen zu anderen Menschen oder Institutionen (Rotter, 1967). Die Frage ist nun, ob es möglich ist, dieses unterschiedliche Vertrauensverhalten zu clustern und Typen zu bilden. Unterschiedliche Vertrauenstypen haben ein differenziertes Vorschussvertrauen und gehen somit anders in mögliche Transaktionssituationen hinein. Jede Transaktionsabsicht wird dabei vom bereits vorhandenen Vertrauen oder

Misstrauen eines Nutzers beeinflusst. Deshalb wird in dieser Dissertation bei der Identifikation von unterschiedlichen Vertrauenstypen im Internet eine Ex-ante-Perspektive eingenommen. Durch eine breit angelegte Online-Umfrage sollen Vertrauenstypen im Internet identifiziert werden. Durch Vertrauensindikatoren, persönliche Eigenschaften und demografische Faktoren sollen diese charakterisiert werden, um Aussagen über deren Vertrauensverhalten in möglichen Transaktionen ableiten zu können.

Forschungsfrage 2:

Sind während einer Transaktion im Internet für die unterschiedlichen Vertrauenstypen dieselben Vertrauensfaktoren relevant?

Ziel ist es, herauszufinden, ob während einer Transaktion pro Vertrauenstyp die gleichen vertrauensfördernden Faktoren relevant sind oder ob die unterschiedlichen Typen auf andere Vertrauensindizien reagieren. Auf diese Weise können Aussagen darüber gemacht werden, welcher Vertrauenstyp im Internet während einer Transaktion auf welche Vertrauensindikatoren achtet. Dadurch wird es möglich, praxisgerechte Massnahmen für Anbieter von Online-Geschäftsmodellen abzuleiten, um das Vertrauen der Nutzer während einer Transaktion zu fördern.

Forschungsfrage 3:

Unterscheiden sich die Vertrauenstypen in Bezug auf ihre Vertrauensabsichten?

Die dritte Forschungsfrage geht der Frage nach, inwiefern Vertrauen als Resultat vorangegangener Transaktionen betrachtet werden kann. Ist eine erneute Transaktion wahrscheinlich? Unterscheiden sich die zukünftigen Verhaltensweisen pro Vertrauenstyp? Durch die Identifikation derjenigen Typen, welche dem Anbieter gegenüber positive Vertrauensabsichten aufweisen, können Schlussfolgerungen für den Aufbau und die Pflege von Nutzerbeziehungen abgeleitet werden.

Das übergeordnete Forschungsziel und die drei Forschungsfragen dieser Dissertation sind in Abbildung 1 grafisch zusammengefasst:

Übergeordnetes Forschungsziel Personengruppen im Internet nach ihren Vertrauenseigenschaften in Typen zu unterscheiden.	
Forschungsfrage 1 (Ex ante)	Existieren bei Internetnutzern unterschiedliche Vertrauenstypen?
Forschungsfrage 2 (In situ)	Sind während einer Transaktion im Internet für die unterschiedlichen Vertrauenstypen dieselben Vertrauensfaktoren relevant?
Forschungsfrage 3 (Ex post)	Unterscheiden sich die Vertrauenstypen in Bezug auf ihre Vertrauensabsichten?

Abbildung 1: Übergeordnetes Forschungsziel und Forschungsfragen der Dissertation (eigene Darstellung)

Diese Fragen bilden ein Dreieck aus empirischem Zugang, Theoriefundierung sowie praktischer Relevanz. Diese Arbeit stellt sich demnach der Aufgabe, die Wirkungszusammenhänge von Vertrauen während des Entscheidungsfindungsprozess pro Vertrauenstyp zu ermitteln, um so Handlungsempfehlungen für Anbieter von Online-Geschäftsmodellen abzuleiten. Kenntnisse über die zukünftigen Vertrauensabsichten der Nutzer ermöglichen es dem Anbieter, zielgruppenspezifisch in den Aufbau und Pflege von Nutzerbeziehungen zu investieren.

1.2.2 Wissenschaftliche Relevanz und Forschungslücke

Vorhergehende Studien haben sich dem Thema persönliche Daten und Privacy im Internet aus verschiedenen Blickwinkeln heraus genähert. Es entstanden Forschungsarbeiten und Publikationen über Konsumentenbedenken in Bezug auf die Datensicherheit (Culnan & Armstrong, 1999; Milne & Boza, 1999), darüber, wie Kunden auf diese Bedenken reagieren (Sheehan & Hoy, 1999), über die Bereitschaft der Kunden, persönliche Daten zur Verfügung zu stellen (Phelps, Nowak & Ferrell, 2000), über das Wissen der Nutzer zum Thema Privacy (Culnan, 1995; Milne & Rohm, 2000) sowie über den Einfluss von Vertrauen auf die Bereitschaft, persönliche Daten zur Verfügung zu stellen (Schoenbachler & Gordon, 2002). Die zentrale Rolle des Vertrauens im Online-Kontext bewog Forscher verschiedener Fachrichtungen,

sich diesem Thema auf empirischer Ebene anzunehmen. Vertrauen im Internet ist jedoch noch immer ein unzureichend untersuchtes Phänomen (Urban et al., 2009). Bislang wurden vorwiegend quantitative Untersuchungen durchgeführt, welche den Einfluss von Vertrauen auf das Verhalten im Internet zum Gegenstand haben (Jarvenpaa, Tractinsky & Vitale, 2000; Yoon, 2002; Schlosser, White & Lloyd, 2006). Einzelne Studien haben Vertrauen in spezifischen Geschäftsfeldern, zum Beispiel Online-Apotheken (Schulz, Büttner & Silberer, 2008) oder Online-Banking (Kim & Moon, 1998), erforscht. Weniger Beachtung wurde jedoch der Frage geschenkt, wie Vertrauen im Internetkontext entsteht, wie es sich entwickelt und wie es gefördert werden kann (Kim, Xu & Koh, 2004; Urban et al., 2009). Gemessen an der grossen Bedeutung von Vertrauen bei Online-Transaktionen wurde Vertrauen im Internet bislang aus akademischer Sicht vernachlässigt.

Bis heute wurden die folgenden Forschungslücken nicht wissenschaftlich aufgearbeitet: Um die unterschiedlichen Nutzer digitaler Geschäftsmodelle besser verstehen zu können, ist es wichtig, sie in idealtypische Cluster zu unterteilen. Nicht alle Nutzer vertrauen der Institution Internet, dem Online-Anbieter oder anderen Menschen in gleichem Masse. Durch die Identifikation unterschiedlicher Typen können differenziertere Analysen und Aussagen über ihr mögliches Verhalten gemacht werden. Ausserdem ist wichtig zu wissen, an welcher Stelle im Entscheidungsfindungsprozess sich der Nutzer befindet. Nutzer steigen mit unterschiedlichem Vorschussvertrauen in eine Transaktion ein (ex ante), achten während der Transaktion auf unterschiedliche Indikatoren zur Beurteilung der Vertrauenswürdigkeit des Anbieters (in situ) und weisen ebenso unterschiedliche Vertrauensabsichten nach einer Transaktion auf (ex post). Neben der Identifikation von Vertrauenstypen soll deshalb geprüft werden, welche Faktoren während einer Interaktion mit dem Anbieter den stärksten Einfluss auf das Nutzervertrauen ausüben. Weiter soll diese Dissertation untersuchen, ob Vertrauen als Resultat vergangener Transaktionen betrachtet werden kann. Der Autorin sind Studien, welche diese Forschungsbereiche wissenschaftlich untersuchen, bis zum heutigen Zeitpunkt unbekannt.

Diese Forschungslücken liefern die Grundlage für diese Dissertation, welche das Vertrauenskonstrukt im Online-Bereich empirisch weiterentwickeln möchte. Dies soll aufgrund einer Überprüfung der in der Literatur meistgenannten Vertrauensfaktoren anhand eines qualitativen Ansatzes erfolgen und danach anhand einer breit angelegten quantitativen Online-Umfrage ausgewertet werden. Vom wissenschaftli-

chen Standpunkt aus soll die Untersuchung zur gegenwärtigen Forschung in den Bereichen Veröffentlichung privater Daten, Privacy und Privacybedenken, Vertrauensmanagement sowie Unternehmenskommunikation im Internetkontext beitragen. Weiter soll die bestehende Literatur, welche Vertrauen hauptsächlich aus der Marketingperspektive beleuchtet (Milne & Boza, 1999; Milne, 2000; Phelps et al., 2000; Phelps et al., 2001; Chellappa & Sin, 2005), um eine ganzheitliche Betrachtungsweise ergänzt werden. Ein Beitrag dieser Dissertation ist die Analyse von Vertrauen im Kontext des Online-Entscheidungsfindungsprozesses. Diese Einbindung in die Vertrauensbildung macht es möglich, den dynamischen Aspekt von Vertrauen in die Untersuchung zu integrieren. Aus der wissenschaftlichen Fachliteratur und aus empirischen Resultaten sollen somit Implikationen für den Umgang mit persönlichen Daten und Vertrauen während des Entscheidungsfindungsprozesses im Internet abgeleitet werden, um so zu einem tieferen Verständnis von Vertrauen im Internet beizutragen.

1.2.3 Praktische Relevanz

Anbieter von Online-Geschäftsmodellen stehen vor der Herausforderung, dass Kunden im Internet ein höheres Risiko als in traditionellen Vertriebskanälen wahrnehmen und dass somit die Wahrscheinlichkeit kleiner ist, dass sie sich auf eine Transaktion einlassen (Premazzi, Castaldo, Grosso, Roman, Brudvig & Hofacker, 2010; van den Poel & Leunis, 1999). In der Offline-Welt ist bereits lange bekannt, dass Kunden nicht gleich Kunden sind. Das gilt auch für Nutzer im Internet und somit für die an diese Nutzer gerichtete Kommunikation. Aus praktischer Sicht fehlen empirisch begründete Handlungsempfehlungen für ein ganzheitliches, den Entscheidungsfindungsprozess einbeziehendes Vertrauensmanagement.

Vertrauen weist eine hohe Relevanz für Wissenschaft und Praxis auf. Die mediale Präsenz von Datenschutzskandalen – wie zum Beispiel der um die Deutsche Telekom oder der um die Deutsche Bahn – zeigt, dass Datensicherheit, Privacy und Vertrauen relevante Themen in unserer Gesellschaft sind (Hoffmann & von Kaenel, 2009). Die kürzlich entbrannten Debatten über die Nutzungsrechte individueller Daten auf Facebook oder Google Street View unterstreichen die praktische Relevanz des Themas. Für Transaktionen im Internet ist das Vertrauen der Nutzer zu einer elementaren Grundvoraussetzung geworden.

Diese Dissertation ermöglicht es Praktikern zu evaluieren, welchem Vertrauenstyp ihre Nutzer zuzuordnen sind. Wenn Anbieter von Online-Geschäftsmodellen wissen, welcher Vertrauenstyp sich in welcher Phase des Entscheidungsfindungsprozesses befindet, können sie gezielt auf die Bedürfnisse ihrer Nutzer eingehen. Aus praktischer Sicht ist die durchgängige Untersuchung von Vertrauen im Entscheidungsfindungsprozess der Nutzer deshalb notwendig, um die vertrauensbildenden Massnahmen auf den Prozessverlauf abstimmen zu können. Weiter sollen Unternehmen für die möglichen Folgen unüberlegten Handelns mit Nutzerdaten sensibilisiert werden. Die in der Dissertation durchgeführte Forschung ermöglicht es, die empirischen Ergebnisse zu Managementimplikationen zusammenzuführen und damit der Wissenschaft sowie der Praxis einen Erkenntnisgewinn zu erbringen. Durch ein aktives Management des Erfolgsfaktors Vertrauen ist es möglich, auch im Online-Bereich langfristige Beziehungen aufzubauen und zu pflegen.

1.3 Aufbau der Dissertation

Um die in Kapitel 1.2.1 vorgestellten Forschungsfragen beantworten zu können, wurde diese Dissertation in die folgenden fünf Schwerpunkte eingeteilt: Auf ein einleitendes Kapitel folgen die der Dissertation zugrunde liegenden Kernkonzepte, das forschungsmethodische Vorgehen, die Ergebnisse sowie Handlungsempfehlungen im Schlussteil. Am Ende dieser Arbeit befinden sich das Literaturverzeichnis sowie der Anhang. Die Struktur der Dissertation wird in Abbildung 2 grafisch zusammengefasst und im Folgenden wird der Aufbau der Dissertation im Detail vorgestellt.

1. Einführung in das Thema

Der erste Teil der Arbeit dient der Heranführung des Lesers an das Thema und in die Forschungsproblematik. Das einleitende Kapitel 1.1 ging auf die Problematik der Unsicherheit der Nutzer bei Online-Transaktionen ein und es wurden die Kernpunkte der aktuellen Debatte des Forschungsthemas aufgezeigt. Das folgende Kapitel 1.2 diskutierte die Zielsetzung und die Forschungsfragen des Dissertationsvorhabens (Kapitel 1.2.1) und skizzierte die wissenschaftliche (Kapitel 1.2.2) und praktische Relevanz (Kapitel 1.2.3) des Dissertationsvorhabens. In diesem Kapitel 1.3 wird der Aufbau der Dissertation vorgestellt und im Kapitel 1.4 wird abschliessend das Forschungsthema abgegrenzt.

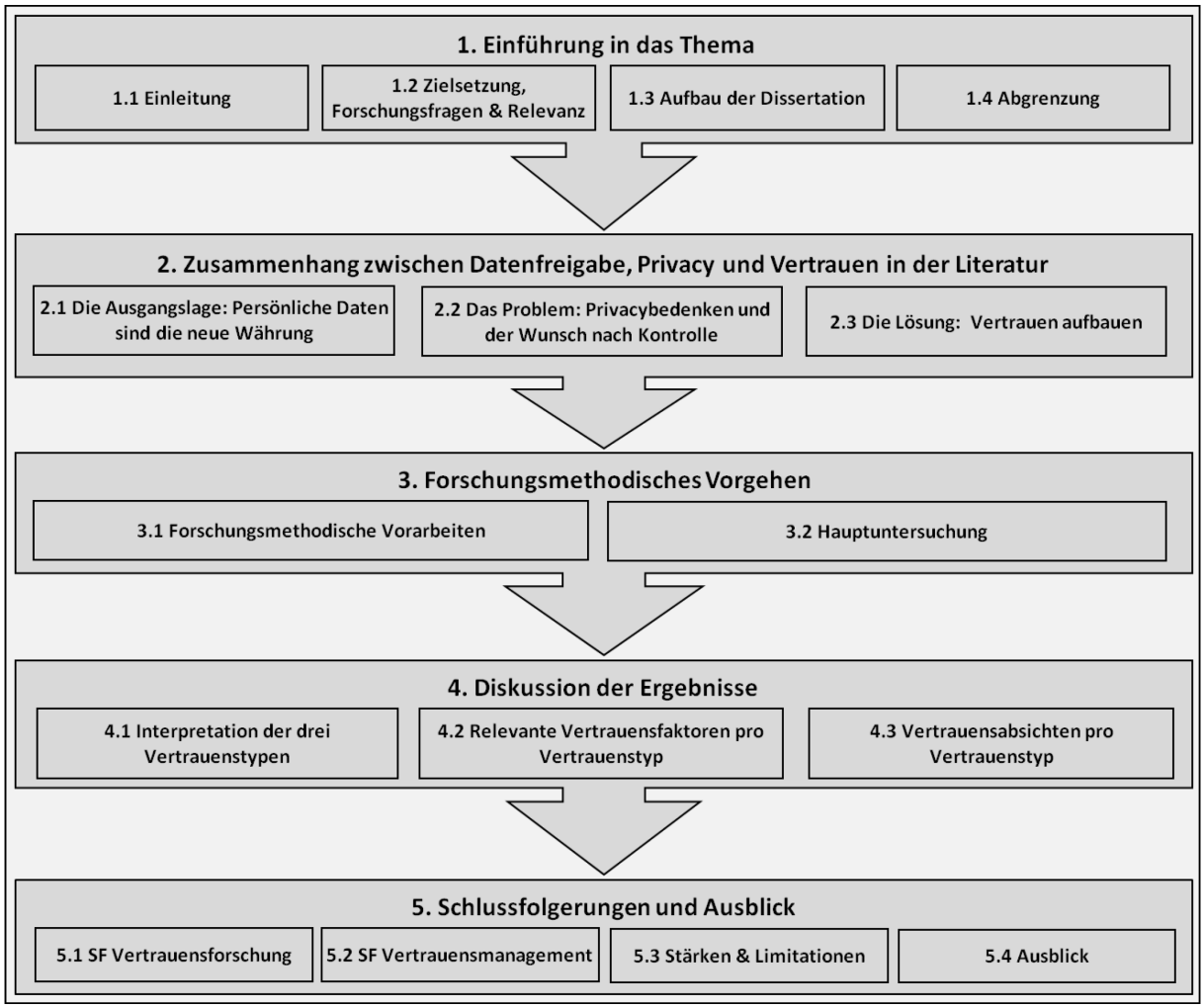


Abbildung 2: Struktur der Dissertation (eigene Darstellung)

2. Zusammenhang zwischen Datenfreigabe, Privacy und Vertrauen in der Literatur

Dieses Kapitel fasst die wesentlichen theoretischen und konzeptionellen Grundlagen der Dissertation zusammen, stellt sie in einen übergeordneten Zusammenhang und gibt einen Überblick über den aktuellen Stand der Forschung. Die relevante Literatur wurde in die drei Bereiche Daten als Währung, Privacy und Vertrauen aufgeteilt. Die Definition dieser Konzepte ist eine wesentliche Grundlage für diese Studie, um eine klare und eindeutige Auseinandersetzung mit der Thematik zu ermöglichen. Die Literatursuche wurde während der vier Jahre dauernden Forschungstätigkeit so lange weitergeführt, bis keine neuen wissenschaftlichen Artikel mit neuen Erkenntnissen zum Thema mehr identifiziert werden konnten.

Im ersten Kapitel 2.1 wird die Ausgangslage diskutiert und beleuchtet, weshalb Daten die neue Währung im Internet sind. Weiter werden die durch das Internet geschaffenen neuen Rahmenbedingungen für Wirtschaft und Gesellschaft erläutert. Das Kapitel 2.1.1 widmet sich den neuen Geschäftsmodellen im Internet und diskutiert deren wesentliche Herausforderungen. Das Kapitel 2.1.2 liefert einen Literaturüberblick über die Bereitschaft der Nutzer, persönliche Daten bereitzustellen, um an Online-Transaktionen teilnehmen zu können. Der Entscheidungsfindungsprozess bei Online-Transaktionen ist Gegenstand des Kapitels 2.1.3. Das Kapitel 2.1.4 fasst die wesentlichen Erkenntnisse zusammen.

Im zweiten Kapitel 2.2 wird detailliert auf das Konstrukt Privacy[2] und das Problem nutzerseitiger Privacybedenken eingegangen. Das Kapitel 2.2.1 beginnt mit der Entstehungsgeschichte und der Definition von Privacy und diskutiert das Bedürfnis eines Individuums nach Privacy. Danach wird im Kapitel 2.2.2 vertieft auf die Bedeutung von Privacy im Internetzeitalter eingegangen, um im letzten Kapitel 2.2.3 auf die Einflussfaktoren von Privacybedenken und auf die Strategien zum Schutz der Privacy einzugehen. Im Kapitel 2.2.4 werden die Erkenntnisse zusammengefasst.

Der dritte Teil der Literaturrecherche (Kapitel 2.3) widmet sich der Lösung des Problems und ergründet das Online-Nutzervertrauen. Im Einleitungskapitel 2.3.1 wird der Fokus zuerst auf die definitorische Abgrenzung von Vertrauen gelegt und die Bedeutung von Vertrauen für Anbieter von Online-Geschäftsmodellen diskutiert. Die Entstehung von Vertrauen sowie die zentralen Einflussfaktoren auf Vertrauen sind Gegenstand des Kapitels 2.3.2. Das Kapitel 2.3.3 betrachtet Vertrauen als Ergebnis eines dynamischen Prozesses und diskutiert die Absicht, in Zukunft zu Vertrauen. Auch dieses Kapitel schliesst mit einer Zusammenfassung (Kapitel 2.3.4).

3. Forschungsmethodisches Vorgehen

Dieses Kapitel erläutert die Vorbereitung und die Durchführung der empirischen Erhebung, um darauf aufbauend die drei im Kapitel 1.2.1 vorgestellten Forschungsfragen zu beantworten, und präsentiert die ersten Resultate der Untersuchung. Dieses Kapitel wird in zwei Bereiche aufgeteilt: in die forschungsmethodischen Vorarbeiten (Kapitel 3.1) sowie in die Hauptuntersuchung (Kapitel 3.2).

---

[2] In dieser Arbeit wird ausschliesslich der englische Begriff Privacy verwendet, da er Privatheit, Privatsphäre, Privatbereich, aber auch Datenschutz beinhaltet.

Das Kapitel 3.1 erläutert die für die Beantwortung der Forschungsfragen nötigen forschungsmethodischen Vorarbeiten im qualitativen und quantitativen Bereich. Im ersten Kapitel 3.1.1 werden die qualitativen Interviews mit Anbietern und Nutzern von Online-Geschäftsmodellen erläutert und deren Auswertung beschrieben. Diese qualitative Phase dient dazu, die aus der Theorie identifizierten nutzerseitigen Vertrauensfaktoren aus Sicht der Anbieter und aus Sicht der Nutzer selbst zu differenzieren und zu ergänzen. Zusammen mit den in der Literaturrecherche identifizierten Faktoren wird in Kapitel 3.1.2 der Online-Fragebogen konzipiert und die Befragung durchgeführt. Im Kapitel 3.1.3 wird der Untersuchungskontext erläutert und im Kapitel 3.1.4 werden anhand von Faktorenanalysen das Vertrauensmass sowie die relevanten Vertrauensfaktoren aus Sicht der Nutzer identifiziert, welche in der Hauptuntersuchung erneut aufgegriffen werden. Im Kapitel 3.1.5 werden die zentralen Erkenntnisse der forschungsmethodischen Vorarbeiten zusammengefasst.

In der Hauptuntersuchung im Kapitel 3.2 werden die verwendeten methodischen Verfahren vorgestellt, durchgeführt und erläutert. Für die Identifikation der Vertrauenstypen werden im Kapitel 3.2.1 die Clusteranalyse und die Diskriminanzanalyse herangezogen; für die Identifikation der relevanten Vertrauensfaktoren (Kapitel 3.2.2) sowie der Vertrauensabsichten (Kapitel 3.2.3) wird jeweils ein Mittelwertvergleich angewendet. Zum Schluss werden in Kapitel 3.2.4 die zentralen Erkenntnisse der Hauptuntersuchung nochmals zusammengefasst.

4. Diskussion der Ergebnisse

Dieses Kapitel bildet das Kernstück der Dissertation. Es widmet sich der ausführlichen Analyse der Ergebnisse des Methodenkapitels und beantwortet die drei in Kapitel 1.2.1 vorgestellten Forschungsfragen. Im ersten Kapitel 4.1 werden die drei identifizierten Vertrauenstypen (Kapitel 4.1.1 / 4.1.2 / 4.1.3) detailliert beschrieben, interpretiert und charakterisiert. Im Kapitel 4.1.4 werden die drei Typen einander gegenübergestellt und benannt. Im zweiten Kapitel 4.2 werden die relevanten Vertrauensfaktoren pro Vertrauenstyp (Kapitel 4.2.1 / 4.2.2 / 4.2.3) im Detail erörtert und diskutiert. Im Kapitel 4.3 werden die Vertrauensabsichten pro Vertrauenstyp (Kapitel 4.3.1 / 4.3.2 / 4.3.3) besprochen und zuletzt werden die wesentlichen Erkenntnisse der drei Forschungsfragen im Kapitel 4.4 zusammengefasst.

5. Schlussfolgerung und Ausblick

Dieses abschliessende Kapitel beinhaltet die Zusammenfassung der Dissertation und Schlussfolgerungen der Vertrauensforschung. Das Kapitel 5.1 ist an die wissenschaftliche Gemeinschaft gerichtet. Darin werden die theoretischen und die empirischen Erkenntnisse dieser Dissertation reflektiert und die Ergebnisse der Untersuchung zusammengefasst (Kapitel 5.1.1 / 5.1.2 / 5.1.3).

Danach wird im Kapitel 5.2 auf die Schlussfolgerungen für das Vertrauensmanagement eingegangen, welche an Wirtschaftsakteure gerichtet sind. Im Kapitel 5.2.1 werden die zentralen Erkenntnisse der Dissertation vorgestellt und im Kapitel 5.2.2 werden konkrete Handlungsempfehlungen für Anbieter von Online-Geschäftsmodellen vorgestellt.

Darauf folgen die Stärken und Limitationen des Forschungsvorhabens (Kapitel 5.3). Geschlossen wird diese Dissertation mit dem Ausblick (Kapitel 5.4), in dem weitere Forschungsmöglichkeiten aufgezeigt werden (Kapitel 5.4.1) und ein Blick in die Zukunft der Privacy- und Vertrauensdebatte gewagt wird (Kapitel 5.4.2).

1.4 Abgrenzung und Einschränkung der Thematik

Die im Kapitel 1.2.1 definierten Forschungsfragen bilden den Rahmen dieser Dissertation und gehen notwendigerweise mit einer Begrenzung der Thematik einher, welche in diesem Kapitel vorgenommen wird. In diesem Sinne soll die vorliegende Arbeit nicht als abschliessende Diskussion des Themas Vertrauensmanagement im Online-Bereich verstanden werden, sondern vielmehr als eine vertiefte Betrachtung eines Teilgebiets davon. Folgende Einschränkungen zu dieser Dissertation und der Übertragbarkeit der Forschungsergebnisse sind zu beachten:

- **Umfang Literaturüberblick Soziale Medien:** Diese Dissertation beleuchtet das Thema Vertrauensmanagement im Online-Bereich. Diese Arbeit ist kein weiterer Bericht über die Entstehung und Entwicklung des Internets und der Sozialen Medien, eine definitorische und konzeptionelle Diskussion aller Begriffe und Konzepte im neuen Internet würde den Rahmen dieser Dissertation bei Weitem sprengen. Deshalb werden nur die grundlegendsten Begriffe, die für das weitere Verständnis dieser Arbeit benötigt werden, diskutiert.
- **Onliner vs. Offliner:** Die geführten Interviews mit Experten und Nutzern von Online-Geschäftsmodellen sowie die Online-Befragung beschränken sich auf Personen, welche das Internet bereits nutzen und adaptiert haben. Diese Studie beruht darauf, Personengruppen im Internet nach ihren Vertrauenseigenschaften in Typen zu unterscheiden. Dieses Forschungsziel ist nur mit Personen erreichbar, die das Internet bereits nutzen. Ziel der Anbieter von Online-Geschäftsmodellen sollte es aber ebenfalls sein, Nicht-Nutzer zu Nutzern zu machen. Es wäre daher sinnvoll, den Forschungsansatz auf Nicht-Internet-Nutzer auszuweiten. Für die Wissenschaft wie auch die Praxis wäre es interessant zu sehen, aus welchen Gründen das Internet nicht genutzt wird und welche Stellhebel betätigt werden müssen, um Nicht-Nutzer zur Nutzung zu bewegen.
- **Geografischer und kultureller Rahmen:** Die empirische Datenerhebung für die Dissertation wurde mit Online-Anbietern vorgenommen, die auf dem deutschen Markt aktiv sind. Ebenso wurden die qualitativen Interviews wie auch die quantitative Online-Befragungen mit Nutzern in Deutschland durchgeführt. Die Internetnutzung, das Verständnis von Privacy sowie Privacybedenken und die Bereitschaft zu vertrauen, können zwischen geografischen und kulturellen

Regionen stark voneinander abweichen. Johnson und Auh (1998) zum Beispiel vertreten die Ansicht, dass die Vertrauensneigung zwischen den Kulturen stark variiert und dass Menschen, die in einer höheren Vertrauenskultur (gemäss Fukuyama (1995) zum Beispiel Deutschland oder Japan) leben, eher bereit sind Vertrauensbeziehungen einzugehen als Menschen, die in niedrigeren Vertrauenskulturen leben (gemäss Fukuyama (1995) zum Beispiel Italien oder China) (siehe dazu auch Zhou & Tian, 2010). Die Ergebnisse und Handlungsempfehlungen der Dissertation sind somit nur begrenzt und unter Berücksichtigung eventueller Kulturunterschiede auf andere Regionen übertragbar.

- **Definition Privacy:** In öffentlichen Debatten wird zwischen Datenschutz und Privacy kaum unterschieden, obwohl es sich dabei um unterschiedliche Konzepte handelt. Datenschutz umfasst juristische, technische und organisatorische Massnahmen, welche die Privacy ermöglichen und schützen helfen. Der Begriff Privacy impliziert Selbstbestimmung, Bürgerrechte und Autonomie der Individuen (Drüeke & Weber, 2007). Da dies eine wirtschaftswissenschaftliche und keine rechtswissenschaftliche Arbeit ist, wird das Verständnis von Privacy aus der öffentlichen Debatte verwendet. Einstellungen und Bedenken bezüglich Privacy sowie das Gerechtigkeitsempfinden sind sehr stark mit dem zugrunde liegenden Rechtssystem und dem politischen System verbunden. In der Dissertation werden die wichtigsten Aspekte der rechtlichen Situation beleuchtet. Auf eine vertiefte Behandlung wird jedoch verzichtet, da dies das Fachgebiet der Autorin überschreiten würde.
- **Untersuchungskontext:** Unterschiedliche Faktoren können die Privacybedenken und das Vertrauen der Nutzer beeinflussen, wie zum Beispiel persönliche Erfahrungen, soziodemografische Faktoren oder der kulturelle Hintergrund. Diese Faktoren liegen aber ausserhalb des Wirkungskreises der Unternehmen. In dieser Arbeit werden diejenigen Faktoren fokussiert und vertieft betrachtet, welche vom Unternehmen direkt oder indirekt gesteuert und beeinflusst werden können.
- **Monetäre Auswirkungen von Vertrauen:** Interessant wäre es, die wirtschaftlichen Auswirkungen von Vertrauen auf Unternehmen zu erforschen und abzuschätzen. Insbesondere die Reduktion der Transaktionskosten durch Vertrauen könnte berechnet werden, um dadurch dem Management ein fundiertes Argumentationswerkzeug für Investitionen ins Vertrauensmanagement zur Verfügung zu stellen (Sako, 1998; Mohr & Spekman, 1994). Es wird auf die Darstel-

lung der monetären Auswirkungen von Vertrauen verzichtet, weil dies den Rahmen der Arbeit sprengen würde.

- **Weitere Stakeholder:** Der Fokus wird auf die Austauschbeziehung zwischen Anbietern von Online-Geschäftsmodellen sowie jenen Nutzern gelegt, welche die Leistungen potenziell nachfragen. Interessant wäre es auch, den Mitarbeiter als Verstärker ins Zentrum der Recherche zu rücken und zu untersuchen, welche Rolle er als Vermittler einnimmt und welchen Einfluss er auf das Vertrauen der Nutzer hat. Ebenfalls könnte der Einfluss weiterer Stakeholder untersucht werden, wie zum Beispiel derjenige der Lieferanten und Zulieferer. Dieser erweiterte Blick auf das Vertrauensgefüge bei Online-Geschäftsmodellen würde jedoch für diese Arbeit zu weit gehen.
- **TAM:** Das Technology Acceptance Model (TAM) ist ein Modell, welches Aussagen darüber trifft, warum eine Technologie von Personen genutzt wird oder nicht (Davis, 1989; Davis, Bargozzi& Warshaw, 1989; Venkatesh & Morris, 2000). Das TAM hat zum Ziel, die Nutzerakzeptanz bzw. die Ablehnung von neuen computerbasierten Technologien vorherzusagen und zu erklären (Davis et al., 1989). Das Grundmodell identifiziert die wahrgenommene Benutzerfreundlichkeit (perceived ease of use) sowie den wahrgenommenen Nutzen bzw. die Nützlichkeit (perceived usefulness) als Haupttreiber für die Akzeptanz neuer Technologien (Venkatesh, 2000). Die zwei Grundfaktoren Benutzerfreundlichkeit und Nützlichkeit sind direkte Treiber, die einen bedeutenden Einfluss auf externe Variablen wie beispielsweise das Design oder die Gebrauchsabsicht haben. Die Technologieakzeptanz wird in dieser Arbeit durch die Faktoren „Vertrauen in die Institution“ Internet und „Technologie“ abgedeckt und es wird nicht zusätzlich auf das TAM eingegangen.
- **Theorie des Sozialkapitals:** Bei Vertrauen in Menschen und Institutionen wird oft von Sozialkapital in der Beziehung zwischen natürlichen Personen gesprochen (Nahapiet & Ghoshal, 1998). Sozialkapital ist die Gesamtheit der Ressourcen, welche mit sozialen Beziehungen verbunden sind (Bourdieu, 1983), und es herrscht Konsens darüber, dass das soziale Kapital konzeptionell auf sozialen Netzwerken beruht (Coleman, 1988; Putnam, 1993). Sozialkapital konzentriert sich demnach auf die Beziehungsebene und setzt Vertrauen, Kooperation und Reziprozitätsansprüche an das Gegenüber voraus. Da diese Arbeit nicht nur auf die Beziehungsebene fokussiert, wird die Theorie des Sozialkapitals in dieser Arbeit nicht weiter vertieft.

Während des Forschungsprozesses sind viele weitere spannende Themen und durch die Wissenschaft unbeantwortete Fragestellungen aufgetaucht. In dieser Arbeit ist es jedoch nicht möglich, alle Aspekte von Vertrauen im Internet vertieft zu beleuchten. Im Kapitel 5.1 „Schlussfolgerungen für die Vertrauensforschung“ werden deshalb interessante offene Fragestellungen in diesem Bereich thematisiert und weitere Forschungsmöglichkeiten diskutiert.

Im folgenden zweiten Kapitel wird der Zusammenhang in der Literatur zwischen der Offenlegung persönlicher Daten während des Online-Entscheidungsfindungsprozesses sowie Privacy und Vertrauen im Detail diskutiert.

2 Zusammenhang zwischen Datenfreigabe, Privacy und Vertrauen in der Literatur

Dieses Kapitel dient zur Übersicht der in der Dissertation aufgearbeiteten, relevanten Literatur. Das grundlegende Konzept der Literaturrecherche ist dreigeteilt, wie in Abbildung 3 dargestellt: Im ersten Kapitel 2.1 wird die Ausgangslage betrachtet und beleuchtet, weshalb Daten die neue Währung im Internet sind. Im zweiten Kapitel 2.2 wird detailliert auf das Konstrukt Privacy und das Problem nutzerseitiger Privacybedenken eingegangen. Das dritte Kapitel 2.3 widmet sich der Lösung des Problems und ergründet, was Vertrauen ist und wie im Internet Vertrauen aufgebaut werden kann.

Abbildung 3: Grundlegende Konzepte der Literaturrecherche (eigene Darstellung)

2.1 Die Ausgangslage: Persönliche Daten sind die neue Währung

In diesem Kapitel werden die durch die Sozialen Medien geschaffenen neuen Rahmenbedingungen für Wirtschaft und Gesellschaft betrachtet. Die dynamische Weiterentwicklung der Sozialen Medien schafft stetig neue Geschäftsmodelle und stellt Nutzer und Anbieter von Online-Geschäftsmodellen gleichermassen vor neue Herausforderungen (Kapitel 2.1.1). Um an Transaktionen im Web teilnehmen zu können, müssen die Nutzer bereit sein, persönliche Daten zur Verfügung zu stellen. Diese Offenlegung persönlicher Daten im Internet eröffnet wiederum Möglichkeiten für neue Geschäftsmodelle, insbesondere im Bereich der Personalisierung (Kapitel 2.1.2). Wie und weshalb entscheidet sich der Nutzer für einen bestimmten Anbieter im Netz? Die Erforschung des Konsumentenverhaltens und die Entscheidungsfindung der Nutzer ist Gegenstand des Kapitels 2.1.3. In Kapitel 2.1.4 werden die Erkenntnisse zusammengefasst.

2.1.1 Die Sozialen Medien führen zu neuen Geschäftsmodellen

2.1.1.1 Die Entwicklung in den Sozialen Medien stellt die Gesellschaft vor neue Herausforderungen

Die rasante Entwicklung der Sozialen Medien in den vergangenen Jahren hat dazu geführt, dass die Gesellschaft heute vor zahlreichen neuen Herausforderungen steht. Das Internet ist zu einem sozialen Katalysator von umfassender Bedeutung geworden, indem jeder die Möglichkeit hat, Informationen zu verbreiten, Forderungen an Unternehmen heranzutragen und damit womöglich die Einstellungen und das Verhalten anderer zu beeinflussen. Nutzer werden zunehmend unabhängiger von traditionellen Medienkanälen wie Zeitung, Radio und Fernsehen, denn sie beschaffen sich gezielt Informationen von unabhängigen Dritten über das Internet (Bucher, Fieseler & von Kaenel, 2009); ein Trend, den Charlene Li und Josh Bernoff (2008) als „Groundswell“ bezeichnen. Die Autoren argumentieren, dass Menschen zunehmend Technologien dazu nutzen, benötigte immaterielle Informationen sowie physische Gegenstände voneinander zu bekommen und nicht mehr von traditionellen Institutionen wie Unternehmen. Die Sozialen Medien werden häufig dafür gepriesen, einen Beitrag zur erleichterten, flächendeckenden Kommunikation und Vernetzung sowie

zur Erhöhung gesellschaftlicher Transparenz zu leisten (Weinberger, 2000; Ruisinger, 2007).

Die Bezugsgrösse des sich im Internet vollziehenden Diskurses ist eine global vernetzte Gesellschaft, in der weder Informationen noch Interessen an geografischen oder anderen Grenzen scheitern (Fieseler & Meckel, 2009). Menschen verbringen heute immer mehr Zeit im oder mit dem Internet – Arbeit, Kommunikation und Freizeit basieren zunehmend auf einer Vielzahl von Online-Geschäftsmodellen. Durch mobile Endgeräte wird das Internet allgegenwärtig und eine immer grösser werdende Zahl von Unternehmen macht sich dies zu Nutze und stellt Angebote zur Verfügung, damit Nutzer sich untereinander verbinden und Kooperationen eingehen können (Hoffmann & von Kaenel, 2010b; Afuah & Tucci, 2001; Mahadevan, 2000; O'Donnell, 2002; Rust et al., 2002). Die Sozialen Medien führen zu einer fundamentalen Verschiebung hin zu einer Nutzer und Kunden zentrierten Welt, in der Customer–Relationship-Management (CRM) zur Kernaufgabe des E-Business avanciert (Culnan, 2000). Beziehungsaufbau und -pflege setzt aber voraus, dass Unternehmen ihre Kunden und deren Bedürfnisse kennen. Im virtuellen Raum bedeutet dies, dass mittels persönlicher Daten Kundenprofile angelegt werden, um so den Kunden besser einzuschätzen.

Bevor ins Thema persönliche Informationen im Internet eingestiegen und deren Bedeutung diskutiert wird, sollen hier für das weitere Verständnis die Begriffe Web 2.0 und Soziale Medien erläutert werden: Das Web 2.0, auch Soziale Medien genannt, umfasst Internet-Anwendungen und -Plattformen, welche die Nutzer aktiv in die Wertschöpfung einbeziehen – Nutzer können beispielsweise eigene Inhalte, Kommentare, Tags oder Bewertungen beisteuern. Wesentliche Merkmale der Wertschöpfung sind somit Interaktivität, Dezentralität und Dynamik (O'Reilly, 2006; 2007; Kilian, Hass & Walsh, 2007). Eine Grundvoraussetzung für diese interaktive Wertschöpfung im Web 2.0 sind gemeinsame Standards und Konventionen; nur wenn Interoperabilität sichergestellt ist, wird die Zusammenarbeit räumlich und zeitlich verteilter Nutzer überhaupt erst ermöglicht (Kilian et al., 2007).

Vom Vorhergehenden unterscheidet sich dieses neue, soziale Internet vor allem durch mehr Partizipation, mehr Authentizität und mehr nutzergenerierte Inhalte (Ruisinger, 2007). Plattformen des Web 2.0 sind beispielsweise Weblogs, Microblogs, Wikis und Social Networks (Fleck, von Kaenel & Meckel, 2010). Welche Geschäftsmodelle auf diesen Internetplattformen möglich sind, steht im Mittelpunkt des nächsten Kapitels.

2.1.1.2 Warum es wichtig ist, sich Gedanken über Geschäftsmodelle zu machen

Durch das rasante Wachstum der Internettechnologie entstehen immer neue Plattformen und Kanäle, auf denen Unternehmen ihre Produkte und Dienstleistungen anbieten können. Besonders im Bereich der personalisierten Produkte und Dienstleistungen entstehen kontinuierlich innovative Geschäftsmodelle (Montgomery & Smith, 2009; Joinson et al., 2007). Massgeschneiderte Lösungen sind dank einfach programmierbaren Algorithmen ohne grossen Aufwand implementierbar und die Eintrittskosten für Startups sind relativ tief (Fan & Tsai, 2010; Timmers, 2000). In dieser algorithmisch personalisierten Umgebung wird es möglich, aufgrund von vergangenem Nutzerverhalten auf die Zukunft zu schliessen (Meckel, 2011) und dem Nutzer personalisierte Konsumvorschläge zu machen (Chellappa & Sin, 2005), wie dies zum Beispiel beim amerikanischen Online-Versandhaus Amazon der Fall ist. Das rasant wachsende Feld der Personalisierung wird in Kapitel 2.1.2.2 näher beleuchtet. In der Personalisierung liegt eine Chance für Nischenprodukte, die bisher sehr schwierig an spezielle Kundengruppen herangetragen werden konnten. Dieses Kapitel befasst sich mit der Definition und den Komponenten von Geschäftsmodellen im Internet und stellt eine Klassifizierung von Online-Geschäftsmodellen vor.

Die Idee hinter der Geschäftsmodellbildung

Der Grund, weshalb die Geschäftsmodellbildung verfolgt wird, besteht darin, dass relevante Teildisziplinen aus der Betriebswirtschaft aggregiert werden können, um so einen Überblick über die Geschäftsaktivitäten in Modellform zu erlangen (Wirtz, 2001, Breuer & Brenner, 2004). Diese Aggregation ermöglicht es, Komplexität zu reduzieren und die nötigen Kernkompetenzen zu bündeln (Weill & Vitale, 2001). Das Modellieren von Geschäftsideen hilft Unternehmen, Wissen zu sammeln und zu teilen, Prozesse, Finanzströme, Erfolgs- und Misserfolgsfaktoren zu analysieren, Chancen und Risiken zu identifizieren, Strategien und Visionen zu entwickeln und dementsprechend die Prozesse neu zu gestalten (Scheer, Deelamm & Loos, 2003). Weiter steigern sie die Akzeptanz der Stakeholder bei Unternehmensentscheiden (Dubosson-Torbay, Osterwalder & Pigneur, 2002). Breuer und Brenner (2004) weisen darauf hin, dass die Begriffe Strategie und Geschäftsmodell in der Literatur oft synonym verwendet werden, obwohl sie signifikante Unterschiede aufweisen (Magretta, 2002). Abgrenzen kann man diese Begriffe durch ihre zeitliche Gültigkeit: Eine Strategie hat eine langfristige Massnahmenkombination zur Zielerreichung (Porter,

2001). Das Geschäftsmodell hingegen erfasst und beschreibt ein Unternehmensnetzwerk zu einem bestimmten Zeitpunkt (Breuer & Brenner, 2004).

Der in der E-Business-Literatur definierte Begriff „Geschäftsmodell" erlaubt einige unterschiedliche Interpretationen; aber auch in der Praxis besteht keine allgemeingültige Definition. Rappa (2011) formuliert dies auf seiner Homepage folgendermassen: "Business models are perhaps the most discussed and least understood aspect of the web." Gemäss Scheer et al. (2003) lässt sich die Entstehung internetbasierter Geschäftsmodelle anhand dreier Entwicklungsströmungen beschreiben: der Anwendung der Internet-Technologie, der Konkretisierung und Anwendung der virtuellen Organisation sowie der Intermediation und Disintermediation auf internetbasierten Märkten. Das heisst, die Internet-Technologie erlaubt die Einbindung aller Marktteilnehmer in ein Zeit und Raum überwindendes, multimediales und transaktionskostensenkendes Netzwerk vielfältiger Dienste der Informations- und Kommunikationstechnologien. Die lose und ad hoc gekoppelten Prozessstrukturen der virtuellen Organisation führen zu einem Maximum an Flexibilität und einem Minimum an Kosten. Durch die Internet-Technologie ist es gelungen, eine direkte und personalisierte Zugangsmöglichkeit zum Endkunden aufzubauen. Dadurch können Mittler und Zwischenhändler in der Wertschöpfungskette eliminiert werden (Scheer et al., 2003).

In der Literatur findet sich eine Fülle unterschiedlicher Definitionen von Geschäftsmodellen[3]. Im Anhang 7.1.1 dieser Arbeit befindet sich deshalb zur Übersicht eine Tabelle mit Definitionen sowie den unterschiedlichen Kategorien von Geschäftsmodellen. Das Konstrukt der viel zitierten Definition von Timmers (1998) geht weiter als die meisten Geschäftsmodelldefinitionen und schliesst die Architektur der Produkt-, Dienstleistungs- und Informationsflüsse sowie die involvierten Akteure als auch die Beschreibung der Nutzerpotenziale und der Erlösquellen mit ein (Scheer et al., 2003): "An architecture for the product, service and information flows, including a description of the various business actors and their roles; and a description of the potential benefits for the various business actors; and a description of the sources of revenues." (Timmers, 1998, S. 4). Diese Definition wird häufig als Grundlage zur Beschreibung von Geschäftsmodellen herangezogen (vergleiche Google-Zitationen im Anhang 7.1.1). Auch die in dieser Dissertation verwendete Definition von Ge-

[3] In dieser Arbeit werden die Begriffe Online-Geschäftsmodell, Online Business Model und E-Business synonym verwendet.

schäftsmodellen basiert auf der Arbeit von Timmers (1998; 2000), da die Geschäftsmodelle klar nach Nutzen und nach Transaktionspartnern (Business-to-Business oder Business-to-Customer) aufgeteilt werden können.

In diesem Kapitel wurde detailliert aufgezeigt, wie Geschäftsmodelle, insbesondere Online-Geschäftsmodelle, in der wirtschaftswissenschaftlichen Literatur definiert werden. Nun soll betrachtet werden, über welche Hauptkomponenten ein Geschäftsmodell verfügt, welche Klassifizierungen vorgenommen wurden und wie das Konzept der Geschäftsmodelle für diese Dissertation operationalisiert wurde.

2.1.1.3 Hauptkomponenten, Klassifizierung und Operationalisierung von Online-Geschäftsmodellen

Um ein Geschäftsmodell beschreiben und verstehen zu können, müssen zuerst die Hauptkomponenten und Einflussfaktoren analysiert werden. Gemäss Osterwalder und Pigneur (2002; 2010) basiert jedes Geschäftsmodell auf neun gleichwertigen Elementen: die Kunden selbst, das Nutzenversprechen der Unternehmung, die Kommunikations-, Distributions- und Verkaufskanäle, die Kundenbeziehung sowie die Erlösquellen. Ausserdem müssen strategische Partnerschaften eingegangen werden, Schlüsselressourcen und Schwerpunktaktivitäten aufgebaut und die Kostenstruktur analysiert werden, wie in Abbildung 4 zusammenfassend dargestellt.

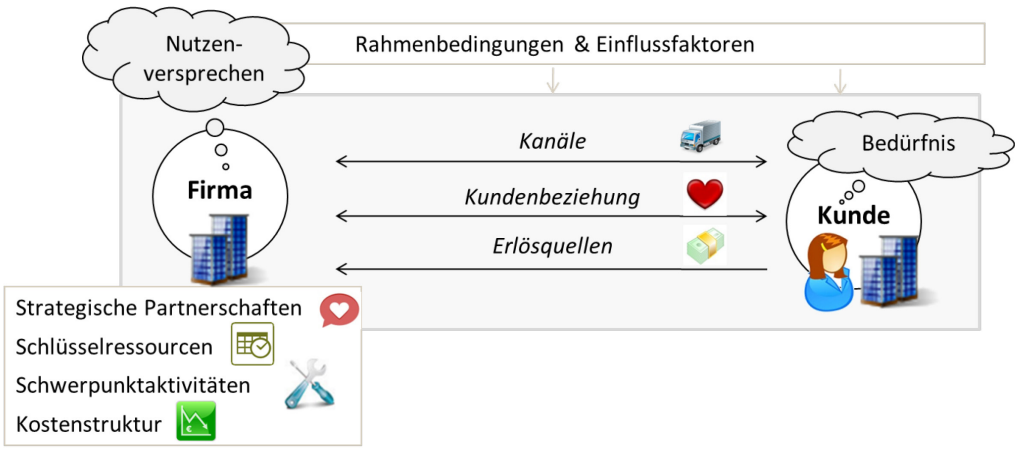


Abbildung 4: Die Hauptkomponenten von Geschäftsmodellen (Osterwalder & Pigneur, 2010; Timmers, 1998; Scheer et al., 2003)

Kunde: Für wen kreieren wir Wert? Die vorhandenen und potenziellen Kunden sind zentrale Bestandteile jedes Geschäftsmodells. Um besser auf die Bedürfnisse

und Wünsche der Kunden eingehen zu können, werden diese in Kundensegmente eingeteilt, Kunden können entweder Geschäftskunden oder Endverbraucher sein. Ein Geschäftsmodell kann eines oder mehrere Kundensegmente bedienen (Osterwalder & Pigneur, 2010; Kotler et al., 2003).

Nutzenversprechen: Welchen Nutzen stiftet das Unternehmen für seine Kunden oder andere Stakeholder? Die Nutzenperspektive beschreibt, welche Bündel von Produkten oder Dienstleistungen angeboten werden, um die Bedürfnisse der einzelnen Kundensegmente zu befriedigen. Sie beschreibt, wie der Nutzen genau aussieht und welchen Beitrag der Nutzer selbst leistet (Osterwalder & Pigneur, 2010; Hoegg, Meckel, Stanoevska-Slabeva & Martignoni, 2006).

Kanäle: Über welche Kanäle erreicht das Unternehmen seine Kunden? Durch das Internet ist es möglich, die Produkte und Dienstleistungen segmentspezifisch zu differenzieren, das heisst, das Unternehmen muss in der Informationsstrategie definieren, welche Kunden über welche Kanäle erreicht werden sollen. Kommunikations-, Distributions- und Verkaufskanäle sind die Schnittstellen zum Kunden, über sie wird das Nutzenversprechen kommuniziert und schlussendlich erfüllt. Diese Kontaktpunkte spielen bei der Entscheidungsfindung und beim Kundenerlebnis eine wichtige Rolle (Osterwalder & Pigneur, 2010).

Kundenbeziehung: Welche Art von Beziehung pflegt das Unternehmen zu welchen Kunden? Diese Komponente beschreibt die Beziehung zu den einzelnen Kundensegmenten. Ziel ist es, eine langanhaltende Kundenbeziehung aufzubauen. Der Aufbau einer Informationsstrategie ermöglicht es dem Unternehmen, den Kunden besser zu verstehen und somit besser auf seine Bedürfnisse eingehen zu können. Unternehmen müssen sich bewusst werden, dass Vertrauen und Loyalität der Kunden zu den wichtigsten Elementen der virtuellen Geschäftswelt geworden sind (Osterwalder & Pigneur, 2010).

Erlösquellen: Wofür sind die Kunden bereit, wie viel zu bezahlen? Erlösquellen können je nach Kundensegment unterschiedlich gestaltet sein und jedem Erlösmodell können andere Preismechanismen zugrunde liegen. Zum Beispiel fixe Preise, Auktionen, Verhandeln, vom Markt oder Volumen abhängige Preise (Dubosson-Torbay et al., 2002; Osterwalder & Pigneur, 2010).

Schlüsselressourcen: Welche Schlüsselressourcen benötigt das Unternehmen, um das gegebene Nutzenversprechen zu erfüllen? Diese Komponente beschreibt, welche Ressourcen vorhanden sein müssen, damit das Geschäftsmodell erfolgreich umge-

setzt werden kann. Schlüsselressourcen können physischer, finanzieller, intellektueller oder menschlicher Natur sein (Osterwalder & Pigneur, 2010).

Schwerpunktaktivitäten: Welche Schwerpunktaktivitäten braucht das Unternehmen um das gegebene Nutzenversprechen umzusetzen? Dieser Abschnitt beschreibt die zentralen Aktivitäten, welche für die Leistungserbringung benötigt werden (Osterwalder & Pigneur, 2010).

Strategische Partnerschaften: Wer sind die wichtigsten Partner, wer die wichtigsten Zulieferer? Immer häufiger werden strategische Partnerschaften ausserhalb des Unternehmens eingegangen, um das Nutzenverspechen bestmöglich erfüllen und einen Mehrwert für den Kunden generieren zu können (Osterwalder & Pigneur, 2010).

Kostenstruktur: Was sind die wichtigsten Kostentreiber? Die Kostenkomponente beinhaltet alle Kosten, welche zur Aufrechterhaltung und Operationalisierung des Geschäftsmodells benötigt werden (Osterwalder & Pigneur, 2010).

Darüber hinaus beeinflussen Rahmenbedingungen wie Konjunktur, Politik, Wettbewerb, Infrastruktur, demografische Faktoren und weitere Einflussfaktoren das Gefüge von Geschäftsmodellen (Scheer et al., 2003). Heute ist es so, dass der Grossteil der Hauptkomponenten in den meisten Geschäftsmodellen im Web 2.0 klar geregelt ist, während das Profit-Modell oft nicht oder ungenügend definiert ist, da die Anbieter exponentiell und organisch gewachsen sind.

Klassifizierung von Online-Geschäftsmodellen

Es gibt viele Möglichkeiten, im Internet Produkte und Dienstleistungen anzubieten. Strategien im Online-Bereich können zum Beispiel für virtuelle Communitys sinnvoll sein, nicht aber für Online-Banking-Angebote und umgekehrt. Um adäquate Strategien entwickeln zu können und Komplexität zu reduzieren, ist es hilfreich, eine Klassifizierung von Online-Geschäftsmodellen vorzunehmen (Lambert, 2006; Bailey, 1994). Wie aus der Tabelle im Anhang 7.1.1 hervorgeht, wurden viele Arbeiten zur Klassifizierung von Geschäftsmodellen verfasst. Dieses Kapitel betrachtet die viel zitierte Klassifizierung nach Timmers (1998; 2000). Er identifiziert darin die elf Geschäftsmodelle E-Shop, E-Procurement, E-Mall, E-Auction, Virtual Community, Collaboration Platform, Third-Party Marketplace, Value-Chain Integrator, Value-Chain Service Provider sowie Information Brokerage und Trust Service, wie in Abbildung 5 ersichtlich.

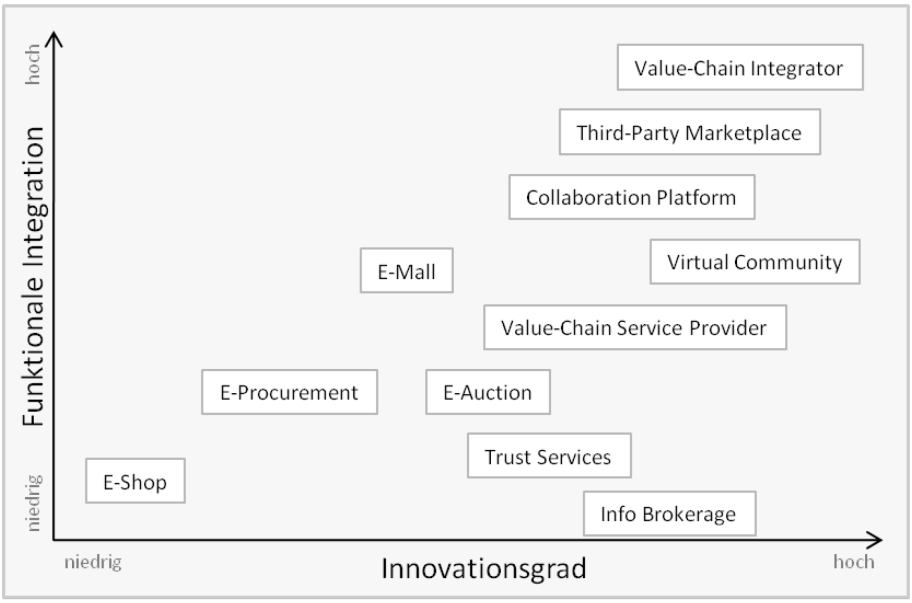


Abbildung 5: Klassifikation von Geschäftsmodellen nach Timmers (1998; 2000)

Timmers (2000) klassifiziert diese elf Geschäftsmodelle anhand zweier Dimensionen. Die erste Dimension ist der Innovationsgrad des Geschäftsmodells, dieser variiert von der elektronischen Version eines traditionellen Geschäfts bis hin zu innovativen Lösungen mittels Informationstechnologien im Wertschöpfungsprozess. Die zweite Dimension ist der Grad der funktionalen Integration. Diese kann von einer einzelnen Funktion wie bei einem E-Shop, welcher nur die Marketingfunktion übernimmt, bis hin zu einer vollständigen Funktionspalette variieren, wie in Abbildung 5 dargestellt ist. Im Anhang 7.1.2 werden diese elf Geschäftsmodelle detailliert beschrieben und voneinander abgegrenzt.

Operationalisierung von Online-Geschäftsmodellen

Da es das Ziel der vorliegenden Dissertation ist, die Bedeutung der auf die Konsumenten gerichteten Kommunikationsmassnahmen zu verstehen, wird eine Systematik angewendet, welche den Fokus auf variierende Angebote für den Kunden legt (Afuah & Tucci, 2001; Timmers, 1998; Mahadevan, 2000; O'Donnell, 2002) und nicht auf Erlösmodelle, Fähigkeiten oder die Organisation selbst (Rappa, 2004; Osterwalder & Pigneur, 2002; Tapscott et al., 2000). Deshalb konzentriert sich die Studie auf Geschäftsmodelle, welche im Business-to-Consumer- (B2C-) oder im Business-to-

Business- (B2B-) Bereich verankert sind und nicht auf Modelle, welche ausschliesslich bei B2B-Transaktionen anwendbar sind (Mahadevan, 2000).

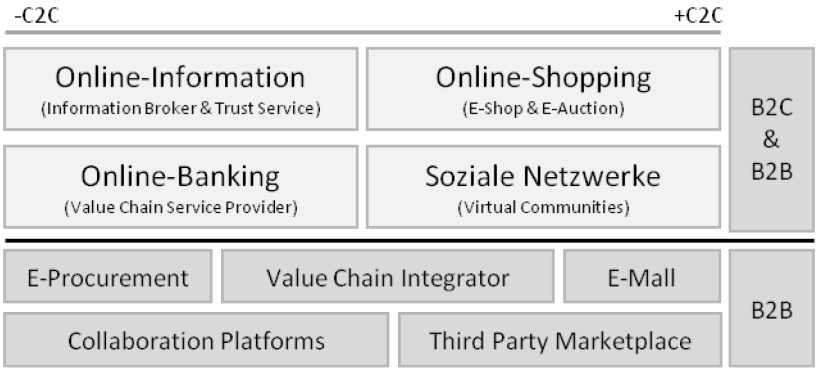


Abbildung 6: Operationalisierung von Online-Geschäftsmodellen (eigene Darstellung)

Wie aus Abbildung 6 hervorgeht, wurde zur Operationalisierung die Kategorisierung von Timmers (1998) aufgespaltet und in reine B2B- sowie in B2C- und B2B-Geschäftsmodelle unterteilt. Die Bereiche E-Procurement, Value Chain Integrator, E-Mall, Collaboration Plattforms sowie Third Party Marketplaces sind in grosser Mehrheit nur in B2B Transaktionen anwendbar und stehen deshalb nicht im Mittelpunkt dieser Dissertation. Der Fokus dieser Arbeit liegt vielmehr in den folgenden vier übergeordneten B2C und B2B Modellen: (1) Online-Information mit den Geschäftsmodellen Information Broker und Trust Services, (2) Online-Shopping mit den Bereichen E-Shop und E-Auction, (3) Online-Banking (als ein Beispiel eines Value Chain Service Providers) und (4) soziale Netzwerke (Virtual Communities). Besonders in den Bereichen Online-Shopping und soziale Netzwerke ist zu beobachten, dass die Transaktionen vermehrt unter den Nutzern selbst stattfinden und sich somit immer häufiger Customer-to-Customer- (C2C-) Geschäftsmodelle abzeichnen.

Wir haben gesehen, dass das partizipative Internet zu neuen Geschäftsmodellen führt und dass viele dieser Geschäftsmodelle auf persönlichen Daten der Nutzer beruhen. Aufgrund der Bedeutung des Offenlegens persönlicher Daten wird diese Thematik im nächsten Kapitel eingehend erläutert.

2.1.2 Wirtschaftsgut Information bei Online-Transaktionen

2.1.2.1 Ohne Daten kein Business

In dieser Arbeit wurde bereits in der Einleitung diskutiert, dass die Bereitschaft der Nutzer, einem Transaktionspartner persönliche Daten zur Verfügung zu stellen, eine notwendige Grundlage für jede Art von Online-Transaktion ist (Culnan & Armstrong, 1999; Milne & Boza, 1999; Eastlick et al., 2006). Diese Bereitschaft ist alles andere als eine Selbstverständlichkeit und muss von den Online-Anbietern als kritischer Erfolgsfaktor betrachtet werden. In der Literatur wird daher mangelndes Vertrauen der Nutzer immer wieder als wesentliches Hindernis für das weitere Wachstum des E-Business genannt (Hoffman et al., 1999a; McKnight et al., 2002a; Urban et al., 2009).

Abbildung 7: Wo wir was über uns enthüllen (eigene Darstellung)

Jedesmal wenn wir uns im Internet bewegen, geben wir persönliche Daten von uns preis, wie in Abbildung 7 beispielhaft dargestellt wird. Sei dies, wenn wir Informationen suchen, einkaufen, Blogs oder Wiki-Einträge lesen und schreiben oder unsere sozialen Kontakte pflegen – alles hinterlässt eine Datenspur (Rust et al., 2002). Die International Data Corporation (IDC) prognostiziert, dass sich die Datenmenge im Internet von 2010 bis 2020 mehr als vervierzigfachen wird (Metzler, 2012). Barrera und Okai (1999) formulieren dies treffend: "To be in cyberspace is to be recorded." (S. 1). Ähnlich wie Geld, Waren oder Dienstleistungen sind persönliche Daten ein Tauschgut, das sich vorab im Verfügungsbereich eines Tauschpartners befindet und im Rahmen der Transaktion gegen einen subjektiven Nutzen eingetauscht wird. Per-

sönliche Daten können daher als ein Äquivalent für die Währung des E-Business[4] verstanden werden (Gasser, 2011).

Neben dem Beziehungsmanagement ist es ein primäres Ziel von Anbietern von sozialen Netzwerken im Internet, die Offenlegung von privaten Daten unter den Nutzern zu fördern und diese darin sogar zu unterstützen (Taraszow et al., 2010). Wie in Abbildung 8 illustriert, versuchen zum Beispiel Inhaber von sozialen Netzwerken bereits bei der Erstanmeldung die Nutzer davon zu überzeugen, dass ihr Profil umso populärer und damit erfolgreicher sein wird, je mehr Informationen sie über sich preisgeben und je aktiver sie sind (Solove, 2007). Nosko, Wood und Molema (2010) konnten in ihrer Studie aufzeigen, dass 25 % der potenziell publizierbaren Daten auf Facebook auch veröffentlicht werden.

Abbildung 8: Anbieter fordern zur Offenlegung privater Daten auf, am Beispiel von Yammer, StudiVZ, Xing und Netlog (eigene Darstellung)

Haben sich Nutzer entschieden, persönliche Daten in eine Transaktion einzubringen, geben sie ihrer Ansicht nach damit keineswegs die Kontrolle über diese auf. Nutzer betrachten persönliche Daten letztlich als eine Art Eigentum und dieses wird durch die Teilnahme an einem Online-Austausch nicht völlig abgetreten (Phelps et al., 2000; Olivero & Lunt, 2004). Die Einforderung persönlicher Daten als Voraussetzung für eine Transaktion berührt daher regelmässig die Privatsphäre der beteiligten Nutzer, was zur Erhöhung der Bedenken bei den Nutzern und Verbrauchern führt (Foxman & Kilcoyne 1993; Phelps et. al., 2000; Chellappa & Sin, 2005): „In fact, it may be quite impossible for customers to transact business on the Internet without reveal-

[4] In der Geschäftsmodellliteratur wird oft auch der Begriff E-Commerce (elektronischer Geschäftsverkehr) verwendet. Unter den Überbegriffen E-Commerce und E-Business wird jede Geschäftsbeziehung verstanden, in welcher Verkäufer und Käufer durch das elektronische Medium Internet geschäftliche Aktivitäten vorbereiten oder ausführen (Guay & Ettwein, 1998; Kotler, Armstrong, Saunders & Wong, 2003).

ing information about themselves that they may be unwilling to share.“ (Rust et al., 2002, S. 455). Mit der Etablierung des Web 2.0 und den damit verbundenen Kommunikations- und Kooperationsformen steigt das Bedürfnis nach einem wirksamen Schutz der Sicherheit und der Privacy der Nutzer (Hoffmann & von Kaenel, 2010b; Urban et al., 2009).

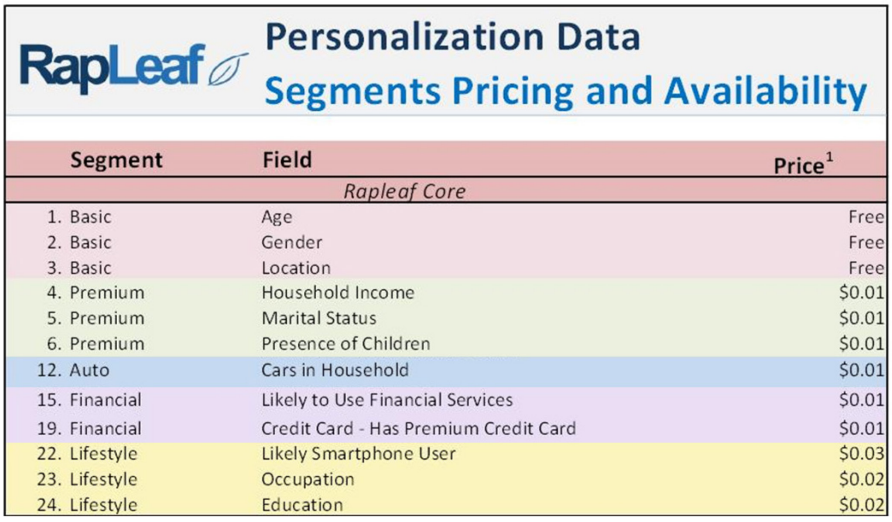
2.1.2.2 Daten sind Business

Die Ökonomisierung personenbezogener Daten hat ihren Durchbruch mit der Etablierung des neuen Internets geschafft, Daten sind der Dreh- und Angelpunkt des Erfolges von Online-Geschäftsmodellen (Gasser, 2011; Krasnova, Spiekermann, Koroleva & Hildebrand, 2010; Rust, Kannan & Peng, 2009; Leonhard, 2011). Die Kosten, die mit der Sammlung und Aufbereitung persönlicher Information verbunden sind, sinken durch die neuen Technologien stetig. Der Wert dieser aggregierten und geclusterten Informationen aber steigt. Unternehmen sind ökonomisch motiviert, immer mehr über ihre Kunden und Nutzer zu erfahren, um mittels digitaler Dossiers[5] trennscharfe Kundensegmentierungen zu ermöglichen, mikrosegmentierte Online-Werbung zu schalten oder direkt mit den Kunden zu kommunizieren (Krasnova et al., 2010). Für ein Unternehmen ist die Sammlung und Aggregation der Daten nur interessant, solange die positiven Effekte (Umsatz, Gewinn) grösser sind als die Kosten (Beschaffungskosten, Datenpflege, Imageverlust). Das Sammeln, Aggregieren, Aufbereiten und der Verkauf personenbezogener Daten im Netz ist heute ein eigenes Geschäftsmodell: “The increasing thirst for personal information spawned the creation of a new industry: the database industry, an information age bazaar where personal data collections are bartered and sold.” (Solove, 2004, S. 19).

“Accurate consumer personal information is one of the most strategic assets of a firm” (Xie, Teo & Wan, 2006, S. 61). Die amerikanische Firma RapLeaf Inc. zum Beispiel verkauft personalisierte Daten und Konsumgewohnheiten zu Namen und E-Mail-Adressen. Mehr als eine Milliarde Adressen, verknüpft mit persönlichen Informationen, sind bereits gespeichert (Soltani, 2011; Schurter, 2011). Diese aggregierten Daten sind im Zeitalter der personalisierten Werbung ein Vermögen wert. Der Blog

[5] “A dossier is a collection of detailed data about an individual. Dossiers are used in European courts to assemble information about a person in order to reach judgement” (Solove, 2004, S. 1).

"The Not-So Private Parts" des Forbes Magazine gab Einblicke in die Preisliste des Data-Mining-Geschäftes (Soltani, 2011). Die Informationen über Haushaltseinkommen oder Zivilstand kosten mit einem US-Cent erstaunlich wenig. Informationen zu Alter, Geschlecht und Wohnort werden gratis dazu geliefert (siehe Abbildung 9). Die berufliche Tätigkeit oder die Information, ob Kinder im Haushalt leben, ist mit zwei Cents bereits doppelt so teuer. Die teuersten Information mit jeweils drei Cent sind gemäss dem Blog des Forbes Magazine der Smartphone-Status, die privaten Interessen, ob der E-Mail-Besitzer Haustiere hat oder ob dieser wohltätige Organisationen unterstützt (Soltani, 2011; Schurter, 2011).[6]



RapLeaf

Personalization Data
Segments Pricing and Availability

Segment	Field	Price[1]
	Rapleaf Core	
1. Basic	Age	Free
2. Basic	Gender	Free
3. Basic	Location	Free
4. Premium	Household Income	$0.01
5. Premium	Marital Status	$0.01
6. Premium	Presence of Children	$0.01
12. Auto	Cars in Household	$0.01
15. Financial	Likely to Use Financial Services	$0.01
19. Financial	Credit Card - Has Premium Credit Card	$0.01
22. Lifestyle	Likely Smartphone User	$0.03
23. Lifestyle	Occupation	$0.02
24. Lifestyle	Education	$0.02

Abbildung 9: Preisliste persönlicher Daten von RapLeaf (Soltani, 2011)

Aus belanglosen Konsumentendaten lassen sich ohne grösseren Aufwand zum Beispiel Alkoholabhängigkeiten, religiöse Zugehörigkeiten oder sexuelle Orientierung bestimmen (Moreno, Vander Stoep, Parks, Zimmerman, Kurth & Christakis, 2009). Oft ist es so, dass der Nutzer selbst diese Informationen zur Verfügung stellt, freiwillig und völlig bewusst (Miyazaki & Fernandez, 2000; Rust et al., 2002) (siehe auch Kapitel 2.1.2.3). Andererseits können Unternehmen durch Cookies[7] und

[6] Zum Vergleich: Das Telefonverzeichnis, die Gelben Seiten sowie das Telefaxverzeichnis der Deutschen Telekom umfasste 281 Bücher, wog 415 kg und kostete ca. 1'450 Euro (Kotler et al., 2003, S. 1099).

[7] Cookies dienen der Archivierung von Informationen auf einem Computer und unterstützen den Austausch von Informationen. Persönliche Daten und die aus den Cookies gewonnen Informationen ermöglichen es den Betreibern von Online-Geschäftsmodellen, genaue Nutzerprofile zu erstellen (Fischer, Keil-Slawik & Richter, 2001).

Clickstream Analysen[8] auch ohne Wissen und Zustimmung der Nutzer Informationen über deren Verhalten sammeln und aggregieren. Auch durch Kooperationen werden zum Beispiel Konsumhistorie-Daten von bestehenden Kunden gegen neue potenzielle Kundendaten getauscht (Miyazaki & Fernandez, 2000).

Die Rohdaten alleine sind aber noch nicht der Schlüssel zum Erfolg, die Informationen müssen zuerst aggregiert und den jeweiligen Zielgruppen zugeordnet werden. Dies ist die natürliche Konsequenz der Verschiebung von Geschäftsmodellen vom Massenmarkt weg hin zur Segmentierung von Märkten, zu Nischenmärkten und zur Personalisierung (Mason, 1986; Richards, 1997; Anderson, 2007)[9]. Deshalb wird im nächsten Kapitel auf die Personalisierung näher eingegangen.

Der Trend zur Personalisierung und zu massgeschneiderten Lösungen

Die Personalisierung von Inhalten ist für Inhaber von Online-Geschäftsmodellen von enormer strategischer Bedeutung (Montgomery & Smith, 2009): "Personalization can be defined as the ability to proactively tailor products and product purchasing experiences to tastes of individual consumers based upon their personal and preference information" (Chellappa & Sin, 2005, S. 181). Personalisierung ist deshalb zwingend von zwei Faktoren abhängig: (1) der Fähigkeit des Verkäufers, Informationen über den Kunden zu erwerben und diese für sich nutzbar zu machen, sowie (2) der Bereitschaft der Kunden, personalisierte Produkte und Dienstleistungen in Anspruch zu nehmen und Informationen zur Verfügung zu stellen (Chelappa & Sin, 2005).

Unternehmen können durch Personalisierung anstatt „One-size-fits-all"-Lösungen mit riesiger Reichweite in Zukunft mehr auf Mikro-Inhalte setzen, welche präzise auf die jeweiligen Zielgruppen abgestimmt sind (Bucher et al., 2009). Besonders für Inhaber von Online-Geschäftsmodellen ist die Personalisierung von enormer strategi-

[8] Unter einer Clickstream-Analyse wird die Rückverfolgung des Navigationspfades und -verhaltens eines Nutzers im Netz verstanden. Dadurch erfahren Unternehmen, wie Nutzer auf ihre Seite gelangen, wo sie sich wie lange aufhalten und können so die Seite optimieren, Prognosen erstellen oder Werbung platzieren (Stolz, 2008).

[9] Anderson (2007) schreibt in seinem Buch „The Long Tail", dass in der Wirtschaft zunehmend eine Bewegung weg vom Massenmarkt hin zu einer Masse von Nischenmärkten stattfindet. Die Theorie des Long Tail besagt, dass nicht mehr eine kleine Anzahl Hits an der Spitze der Nachfragekurve stehen, sondern dass es immer mehr unterschiedliche Produkte oder Dienstleistungen mit kleinen Verkaufszahlen geben wird. Anderson proklamiert durch neue Geschäftsmodelle das Ende der 80/20-Regel.

scher Bedeutung. Personalisierung kann der Erhöhung der Kundenloyalität dienen, kann aber ebenso eine Voraussetzung zur Wettbewerbsfähigkeit sein, da fast jeder Online-Anbieter eine Form von Personalisierung anbietet (Chelappa & Sin, 2005). Die Wichtigkeit von Präferenzinformationen der Kunden ist in der Betriebswirtschaft, insbesondere in der Marketingliteratur, breit dokumentiert (Franke, Keinz & Steger, 2009; Chellappa & Sin, 2005; Montgomery & Smith, 2009). Kenntnisse über die Präferenzen der Kunden sind besonders wichtig für die Kalkulation der Nachfrage, für das Management von Lagerbeständen (Supply Chain Management), um die Beziehung von aktuellen und zukünftigen Partnern einzuschätzen sowie um diskriminierende Preisbildung zu bekämpfen (Blattberg & Deighton, 1991). Die Personalisierung ist für Nischenprodukte, die bisher nur schwierig an spezielle Kundengruppen herangetragen werden konnten, besonders vielversprechend (Bucher et. al., 2009).

Online-Personalisierung wird oft durch Customer-Relationship–Management-(CRM-) Tools in Kombination mit differenzierten Data-Mining-Techniken implementiert. Hoch entwickelte Programme ermöglichen es heute, relativ einfach an grosse Mengen von Kundendaten zu gelangen: Transaktionsdaten, Daten zum Internetverhalten, Bewegungsabläufe und Klicks können nachvollzogen, gespeichert und ausgewertet werden (Culnan & Armstrong, 1999; Metzler, 2012). Diese Systeme tragen Informationen zu Kunden und ihren Präferenzen zusammen, analysieren diese und erstellen so Kundenprofile (Winer, 2001; Chellappa & Sin, 2005; Raghu, Kannan, Rao & Whinston, 2001). Solche individuellen Kundenprofile ermöglichen es den Inhabern von Online-Geschäftsmodellen, Produkte und Dienstleistungen auf einer 1:1-Basis anzubieten, was wiederum die Kundenzufriedenheit, die Kundenloyalität und die Cross–Selling-Möglichkeiten erhöht (Reichheld, 1996; Mittal & Kamakura, 2001). Der Grossteil der Kunden schätzt die Annehmlichkeiten der Personalisierung (Franke et al., 2009). Den grössten Mehrwert bietet das massgeschneiderte Produkt oder die individuelle Dienstleistung an sich. Die durch dieses sogenannte „Profiling“ gespeicherten Daten bedeuten aber auch, dass der Kunde nicht jedesmal seine Daten neu eingeben muss. Name, Adresse und Bankdaten zum Beispiel sind bereits registriert. Zudem werden dadurch zusätzliche Leistungen wie personalisierte Empfehlungen aufgrund des bisherigen Kaufverhaltens, Mengenrabatte, Preisüberwachungen anhand einer persönlichen „Watch List“ oder aber individualisierte Benutzereinstellungen wie Farbe der Homepage oder die Auflistung der Suchresultate ermöglicht (Volokh, 2000; Chellappa & Sin, 2005).

Aus welchen Beweggründen heraus Nutzer und Kunden persönliche Informationen zur Verfügung stellen, wird im nächsten Kapitel thematisiert.

2.1.2.3 Die Offenlegung persönlicher Daten im Internet

Jourard (1971) definiert die Offenlegung persönlicher Daten (self-disclosure) als die Quantität (Breite) und Qualität (Tiefe) der persönlichen Information, welche ein Individuum anderen Personen zur Verfügung stellt. Ebenso definieren Wheeless und Grotz (1976): "Any message about the self that a person communicates to another" (S. 338). Die theoretischen Grundlagen der Offenlegung persönlicher Daten basieren auf der Social-Exchange-Theorie (Blau, 1964; Gouldner, 1960). Die Theorie geht vom Reziprozitätsgedanken aus: Wenn ein Individuum einer anderen Person hilft, erwartet diese im Austausch eine Gegenleistung dafür. Die individuell wahrgenommenen Kosten werden dabei gegen den Nutzen abgewogen (Homans, 1958). Diese Logik bildet die Basis für die Privacy-Calculus-Theorie (Krasnova et al., 2010). Diese besagt, dass der erhaltene Nutzen bei einer Transaktion höher sein muss als das Risiko, welches man durch die Preisgabe der Daten eingeht (Culnan & Armstrong, 1999; Dinev & Hart, 2006).

Persönliche Daten sind Handelsgüter, welche von Marketingfirmen, Versicherungen, Kreditanstalten usw. gekauft und verkauft werden (Xie et al., 2006; Gasser, Cortesi & Palfrey, 2011; Moscardelli & Liston-Heyes, 2004). Trotz dieses Wissens, der Warnungen und Unsicherheit um unsere Privacy geben immer mehr Nutzer persönliche Daten im Internet preis: 75 % aller im Netz vorhandenen Daten werden von den Nutzern selbst generiert (Leonhard, 2011). Welches sind die Einflussfaktoren auf die Bereitschaft, persönliche Daten offenzulegen?

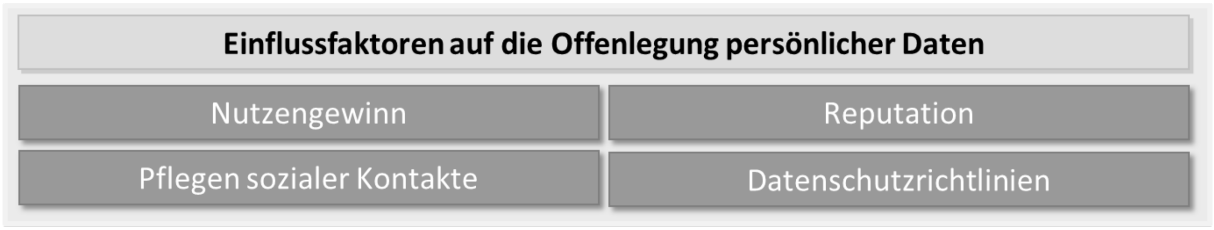


Abbildung 10: Einflussfaktoren auf die Offenlegung persönlicher Daten (eigene Darstellung)

In der Literatur werden der Nutzenaspekt, das Pflegen von sozialen Beziehungen, die Reputation des Unternehmens sowie die proaktive Kommunikation von Datenschutzrichtlinien als Einflussfaktoren auf die Bereitschaft zur Offenlegung persönli-

cher Daten diskutiert (Andrade, Kaltcheva & Weitz, 2002; Xie et al., 2006; Premazzi et al., 2010; Hui, Tan & Goh, 2006), wie in Abbildung 10 dargestellt. Diese vier Einflussfaktoren werden im Folgenden erläutert.

(1) Nutzengewinn wird gegen das Risiko abgewogen: Die Forschung geht davon aus, dass die Bereitschaft der Nutzer, Daten zur Verfügung zu stellen, davon abhängt, wie sie die Kosten, das Risiko oder die Vorteile der Transaktion einschätzen (Andade, Kaltcheva & Weitz, 2002; Premazzi et al., 2010; Im, Lee, Taylor & D'Orazio, 2008; Jacobs, Hyman & McQuitty, 2001). Bei jeder Online-Transaktion müssen die Nutzer abwägen, ob der erwartete Nutzengewinn grösser sein wird als der Umfang der geforderten Daten und somit dem potenziellen Kontrollverlust über diese Daten (Hoffmann & von Kaenel, 2010a; Culnan & Bies, 2003; Chellappa & Shivendu, 2010; Phelps et al., 2000). Der Nutzengewinn kann aus einer Reihe von Vorteilen bestehen: Zeitersparnis, das Nichtvorhandensein von Öffnungszeiten, Anonymität, das Pflegen von sozialen Kontakten, Informationen, Ortsunabhängigkeit, Unterhaltung, Speicherplatz oder Bildung. Krasnova et al. (2010) bezeichnen den Nutzengewinn als den zentralen Faktor bei der Abwägung der Datenpreisgabe. In der Privacy-Literatur wird dieser Trade-off zwischen Bedenken und Datenfreigabe auch als „Privacy Calculus" bezeichnet (Laufer & Wolfe, 1977; Xie et al., 2006; Zhang, Wang & Chen, 2000; Lwin & Williams, 2003; Li, Sarathy & Xu, 2010). Im Online-Umfeld sieht man häufig, dass Unternehmen über gezielte Anreize (z. B. einen Gutschein, Geld, Gewinnchance) an Kundendaten gelangen möchten (Chellappa & Shivendu, 2010). Premazzi et al. (2010) konnten in ihrer Studie aufzeigen, dass Nutzer zwar angeben, dass solche Anreize keinen Einfluss auf die Offenlegung ihrer persönlicher Daten hätten, ihr Verhalten aber Gegenteiliges zeigt. Ausserdem konnte aufgezeigt werden, dass wenn Unternehmen für die Offenlegung persönlicher Daten Anreize zur Verfügung stellen und die Nutzer dem Unternehmen nicht vertrauen, die Nutzer dazu neigen, die Stabilität des Unternehmens in Frage zu stellen (Premazzi et al., 2010; Andrade et al., 2002). Monetäre Belohnungen können Kunden und Nutzer sogar davon abhalten, persönliche Daten offenzulegen (Li et al., 2010). Anreize und Belohnungen können somit einen gegenteiligen Effekt auslösen und sollten vorsichtig eingesetzt werden.

(2) Das Pflegen sozialer Kontakte und die Identitätsbildung im Internet: Für die Nutzer selbst ist das Offenlegen von persönlichen Informationen der Grundstein für das Pflegen sozialer Beziehungen (Christofides, Muise & Desmarqais, 2009). Im täglichen Leben können soziale Merkmale wie Alter, Geschlecht, sozioökonomischer Status oder Bildung Barrieren sein, um neue Beziehungen aufzubauen. Die Anonymität

im Internet, besonders in sozialen Netzwerken, zwingt dazu, potenzielle Beziehungen auf gemeinsamen Interessen aufzubauen statt auf Ähnlichkeiten im sozialen Umfeld (Brashers, Adkins & Meyers, 1994; Mesch & Beker, 2010). Die Sozialen Medien, insbesondere die sozialen Netzwerkseiten ermöglichen es den Nutzern, soziales Kapital zu pflegen und zu akkumulieren (Ellison, Steinfield & Lampe, 2007). Das Offenlegen von persönlichen Daten in einer sozialen Gruppe kann das Vertrauen unter den Mitgliedern fördern und zur Bildung einer Gruppenidentität beitragen (Mesch & Beker, 2010; Galegher, Sproull & Kiesler, 1998). Dadurch können Unsicherheiten reduziert und künftige Verhaltensweisen abgeschätzt werden, was in sozialen Beziehungen fundamental wichtig ist (Heath & Bryant, 2000; Mesch & Beker, 2010). Krasnova et al. (2010) haben festgestellt, dass die Einfachheit der Beziehungspflege im Netz der wichtigste Grund ist, in sozialen Netzwerken persönliche Daten preiszugeben.

Wazlawik, Beavin und Jackson (1969) stellen fest, dass Individuen nicht nicht kommunizieren können[10]. Individuen können sich demnach auch nicht nicht selbst darstellen, besonders nicht in einem Medium, welches jede Bewegung dokumentiert. Jeder eingegebene Suchbegriff, jeder gehörte Song oder jede Statusmeldung zahlt auf das Profil des Nutzers ein und bildet dessen Identität. Die Identität ist die Kombination von Merkmalen, mit denen sich Individuen voneinander unterscheiden lassen (Oerter & Montada, 2002). Um sozial wirksam zu werden, müssen Identitäten nach aussen präsentiert werden, denn Identität entsteht aus den Wechselwirkungen von Eigenwahrnehmung und Fremdbeurteilung (Misoch, 2004). Die Identitätsbildung basiert auf dem Prozess der Selbsterkenntnis und der Selbstgestaltung. Selbsterkenntnis ist die Reflexion über das eigene Selbst und beinhaltet eine kritische Selbstbeobachtung (Oerter & Montada, 2002). Die Nutzung von Anonymität im Internet erlaubt es einem Individuum, gleich mehrere unterschiedliche Identitäten zu kreieren und virtuell zu leben, um so verschiedene Aspekte seiner Persönlichkeit zu leben (Mesch & Beker, 2010; Turkle, 1995). Die Identität einer Person ist aber nicht nur ein individuelles Charakteristikum, sondern auch ein soziales Konstrukt. Die Selbstgestaltung einer Person beinhaltet dementsprechend nicht nur das, was sie selbst über sich nach aussen mitteilt, sondern auch das, was andere über sie sagen und was sie

[10] Die Autoren verstehen jede Art von Verhalten (nonverbal und unbewusst) als eine Form der Kommunikation. Da der Mensch sich nicht nicht verhalten kann, ist es auch unmöglich, nicht zu kommunizieren.

über andere sagt. Das Offenlegen von Information wird dadurch zu einem Instrument der Identitätsgestaltung (Christofides et al., 2009). Goffman (1959) unterstreicht die Wichtigkeit dieser Identitätsgestaltung mit der Aussage, dass eine konsistente Selbstdarstellung und ein positives Image die Grundlage für materiellen und immateriellen Erfolg bilden. Besonders wichtig ist die Identitätsbildung bei Jugendlichen. Heranwachsende müssen sich selbst mit den eigenen Stärken und Schwächen präsentieren, um dadurch Anerkennung und Freunde zu gewinnen und um ein realistisches Selbstbild entwickeln zu können (Krotz, 2009; Boyd, 2007). Dies taten Jugendliche schon immer in ihrem sozialen Umfeld, heute findet diese Identitätsbildung aber zusätzlich im Internet statt (Boyd, 2007; Turkle, 1998; Krotz, 2009; Mesch & Beker, 2010). Palfrey und Gasser (2008) stellen fest, dass Jugendliche heute gar nicht mehr zwischen Online- und Offline-Identität unterscheiden, sondern die beiden Identitäten als eine Einheit betrachten.

(3) Auf die Reputation des Unternehmens kommt es an: Unternehmen können die subjektiven Kosten der Offenlegung privater Daten mindern, indem sie bei den Nutzern Vorschussvertrauen über die Reputation aufbauen (Premazzi et al., 2010; Wang et al., 2004; Koufaris & Hampton-Sosa, 2004; McKnight, Kacmar & Choudhury, 2004; Andrade et al., 2002). "A corporate reputation represents the 'net' affective or emotional reaction – good or bad, weak or strong – of customers, investors, employees, and the general public to the company's name" (Fombrun, 1996, S. 37). Je nach Stakeholdergruppe sind andere bzw. unterschiedlich gewichtete Inhalte der Reputation des Unternehmens bedeutsam (Riordan, Gatewood & Bill, 1997) und unterschiedliche Erwartungen müssen erfüllt werden (Fombrun, 1996). Nutzer schliessen von einer guten Reputation eines Unternehmens darauf, dass die persönlichen Daten sicher und vertrauensvoll verwaltet werden, und sind deshalb bereit, ihre Daten zur Verfügung zu stellen (Gefen & Straub, 2003; Shapiro, 1987; Xie et al., 2006). Bewegen sich Nutzer auf einer Internetseite eines unbekannten Unternehmens, sind die Privacybedenken besonders hoch und dementsprechend ist die Bereitschaft, persönliche Daten zur Verfügung zu stellen, kleiner (Milne & Culnan, 2004).

(4) Kommunikation der Datenschutzrichtlinien: Das Vorhandensein von Datenschutzrichtlinien ist eine Grundvoraussetzung für Online-Anbieter, insbesondere wenn sie auf persönliche Daten ihrer Kunden angewiesen sind (Xie et al., 2006; Milne & Culnan, 2004; Milne & Gordon, 1993; Phelps et al., 2000). Denn haben Nutzer Datenschutzbedenken, konsumieren sie weniger oft und kaufen für kleinere Beträge ein (Milne & Boza, 1999; Phelps et al., 2001; Eastlick et al., 2006). Datenschutzbedenken

haben demnach einen negativen Effekt auf das Nutzer- sowie auf das Kaufverhalten. Aber auch die Bereitschaft, persönliche Informationen preiszugeben, nimmt mit zunehmenden Datenschutzbedenken ab (Schoenbachler & Gordon, 2002; Sheehan & Hoy, 1999; Wang et al., 2004). Anbieter von Online-Geschäftsmodellen versuchen diese Bedenken zu mildern, indem sie beispielsweise Datenschutzerklärungen aufstellen. Datenschutzrichtlinien beinhalten Angaben über den Gebrauch und die Verbreitung aller angegebenen persönlichen Daten und garantieren den Schutz der Privacy (Egger, 2001). Studien haben gezeigt, dass Unternehmen durch Vertrauensbildung Bedenken bezüglich der Privatheit mildern können, indem sie zum Beispiel auf die Fairness ihrer Privacy-Praktiken hinweisen (Culnan & Armstrong, 1999). Die Literatur empfiehlt Unternehmen explizite, transparente und verständliche Datenschutzrichtlinien auszuarbeiten, damit Kunden eine Entscheidungsgrundlage besitzen und dadurch befähigt sind, ihre Rechte auszuüben. Dadurch werden Bedenken bezüglich der Privacy abgeschwächt (Lanier & Saini, 2008; Milne, Culnan & Greene, 2006; Pollach, 2005). Der Glaube daran, dass die Datenschutzerklärung auch eingehalten wird, basiert aber immer auf dem Vertrauen der Nutzer gegenüber dem Unternehmen.

Wie entscheidet ein Nutzer aber, welches Angebot aus welchem Geschäftsmodell er nutzen möchte? Wer mit seinem Online-Geschäftsmodell erfolgreich sein will, sollte wissen, wie sich der Konsument im Internet verhält und wie sein Entscheidungsfindungsprozess aussehen könnte. Der Prozess, wie der Nutzer oder Kunde sich für einen Online-Dienst entscheidet, ist laut Kohli, Devaraj und Mahmood (2004) noch ungenügend erforscht. Das folgende Kapitel geht der Frage nach, wie sich der Konsument im Internet bei einer Entscheidungsfindung verhält.

2.1.3 Die Entscheidungsfindung im Internet

2.1.3.1 Die Erforschung des Konsumentenverhaltens

Das Studium des Konsumentenverhaltens (Consumer Behaviour) ist eine von zwölf zentralen Denkschulen des Marketing (Shaw & Jones, 2005). Die Konsumentenverhaltensforscher befassten sich bereits um 1950 mit Fragestellungen zum Kauf und zur Verwendung von Produkten und Dienstleistungen: Wer kauft? Wie wird gekauft? Wann wird gekauft? Wo wird gekauft? Warum wird gekauft? (Kotler et al., 2003). Die Suche nach Antworten treibt Wissenschaftler und Marketingfachleute seit

Längerem an. Der Psychologe Jacoby (1975) schrieb: "Consumer behavior exists and would continue to exist even if no discipline chose to make it the object of study" (S. 980).

Unternehmen versuchen die Beweggründe der Nutzer für den Kauf eines Produktes oder einer Dienstleistung zu eruieren, um diese steuern und beeinflussen zu können. Für Unternehmen ist es von grosser Bedeutung, möglichst viel über den Kunden und den Verbraucher in Erfahrung zu bringen. Die Konsumentenforschung setzte ihren Fokus in den letzten Jahren vermehrt auf den Prozess, den Konsumenten durchlaufen, um eine Entscheidung (meistens ein Kaufentscheid) zu treffen (Wilson, 1981; Hoyer, 1984; Mittal, 1989; Kohli, et al., 2004; Essoussi & Zahaf, 2009). Im Zentrum dieses Forschungsstrangs steht die Frage, wie der Konsument auf bestimmte Marketingstimuli wie beispielsweise Preise, Werbung, Marke usw. reagiert. Ein Erklärungsversuch liefert das Anreiz-Reaktions-Modell des Konsumentenverhaltens (Kotler et al., 2003). Gemäss Kotler et al. (2003) wirken Marketing und andere Anreize auf den Konsumenten ein und lösen bei ihm eine Reaktion aus[11]. Wie genau Marketinganreize in Reaktionen umgewandelt werden können, ist seit Jahren Gegenstand der Marketingforschung und wird im Modell Black Box genannt. Einerseits wirken die Persönlichkeit und die Aufgeschlossenheit des Käufers darauf, wie die Anreize aufgenommen werden, andererseits wird beim Käufer ein Entscheidungsfindungsprozess angestossen, der sein Verhalten bestimmt und beeinflusst. Was aber genau in dieser Black Box geschieht, muss weiter erforscht werden. Das Konsumentenkaufverhalten werden wir gemäss Kotler et al. (2003) nie vollständig vorhersagen können, die Modelle können uns aber dabei helfen, den Kunden besser zu verstehen. Im nächsten Kapitel soll nun diese Black Box anhand des Problemlösungsprozesses und des Entscheidungsfindungsprozesses näher betrachtet werden.

2.1.3.2 Vom Problemlösungsprozess zum Entscheidungsfindungsprozess

John Dewey entwickelte bereits 1910 einen fünfstufigen Problemlösungsprozess, wie in der linken Grafik in Abbildung 11 dargestellt ist (in Darley, Blankson & Luethge, 2010). Der Prozessanstoss ist die Problemdefinition, danach folgt die Problem-

[11] Die Input-Variablen des Anreiz-Reaktions-Modells werden in der Literatur auch unterteilt in endogene (z. B. sozioökonomische Merkmale) und exogene Einflussfaktoren (z. B. Marketingmassnahmen) (Meffert, 1986; Ergenzinger & Thommen, 2005).

analyse, welche potenzielle Lösungen hervorbringt, die anhand von Auswahlkriterien evaluiert werden. Geschlossen wird der Prozess durch die Implementierung der vom Entscheider wahrgenommenen besten Lösung. Engel, Kollat & Blackwell (1968, 1978) sowie Engel, Blackwell & Miniard (1986) erweitern das Modell von Dewey und wenden es auf das Konsumentenverhalten an (rechte Grafik Abbildung 11).

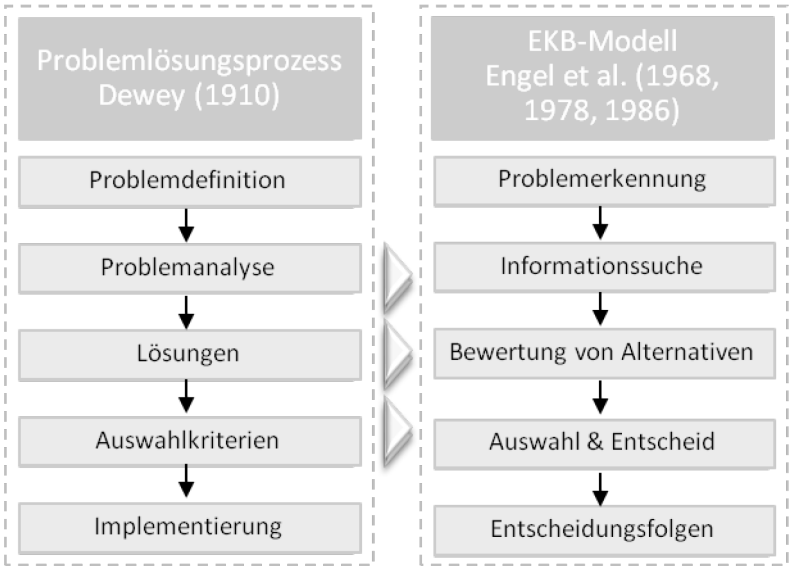


Abbildung 11: Vom Problemlösungs- zum Entscheidungsfindungsprozess (Dewey, 1910; Engel et al., 1968; 1978; 1986)

Der Entscheidungsfindungsprozess des Engel-Kollat-Blackwell-Modells (EKB-Modell) umfasst folgende fünf Kernelemente: Problemerkennung, Informationssuche, Bewertung von Alternativen, Auswahl und Kaufentscheid sowie die Entscheidungsfolgen (Engel et al., 1968, 1978, 1986; Kotler et al., 2003; Solomon, 2004). Im Folgenden werden diese fünf Kernelemente kurz besprochen.

Problemerkennung: In dieser Phase erkennt der Kunde oder der Nutzer ein Problem und das Bedürfnis nach einem Produkt, einer Dienstleistung oder einer Interaktion entsteht. Die Wahrnehmung des Bedarfs kann entweder aufgrund eines internen Anreizes (z. B. Grundbedürfnis) oder eines externen Stimulus (veranlasst durch die Umwelt, z. B. Werbung) beeinflusst werden (Kotler et al., 2003). **Informationssuche:** Nach der Erkenntnis beginnt der Prozess der Informationsgewinnung. Der Kunde beginnt, spezifische Informationen zum Thema zu sammeln. Wie lange und wie intensiv eine Person bereit ist, Informationen zu suchen, hängt vom persönlichen Engagement (high/low involvement) ab (Antil, 1984; Kotler et al., 2003). **Bewertung von Alternativen:** Die durch die Informationssuche gewonnenen Alternativoptionen werden gegeneinander abgewogen und bewertet. Preisvergleiche, Kundeninterakti-

on, Ratings, Empfehlungen, Informationen zur Sicherheit, Foren und Chats oder soziale Netzwerke können für die Bewertung herangezogen werden. **Auswahl und Entscheid:** Aufgrund der ausgewerteten Information wird ein Entscheid getroffen. Der Kunde wählt die für ihn bestbewertete Option aus, welche seiner Meinung nach sein Problem bestmöglich löst oder sein Bedürfnis befriedigt. Der Entscheid kann in einer Transaktion oder einer Interaktion ausgeführt werden.[12] **Entscheidungsfolgen:** Nachdem der Kunde den Prozess der Registrierung und der Zahlungsmodalitäten abgeschlossen hat, das Produkt und die Leistung erhalten und konsumiert hat, überdenkt der Kunde nochmals seine Entscheidungsfindung. War die Entscheidung richtig? Der Kunde vergleicht seine Erwartungen mit der wahrgenommenen Leistung und ist entweder zufrieden oder unzufrieden mit seinem Entscheid (Solomon, 2004; Kotler et al., 2003).

Diese fünf Stufen sind gemäss Darley et al. (2010) die meistakzeptierten Phasen des Entscheidungsfindungsprozesses in der Konsumentenverhaltensforschung (siehe auch Assael, 1998; Blackwell, Miniard, & Engel, 2005; Kotler et al., 2003). Von Interesse ist der gesamte Entscheidungsvorgang beim Käufer und nicht nur der isolierte Kaufentscheid. Der Vorgang des Kaufs beginnt nicht erst mit dem Kauf selbst, sondern schon lange vorher und er wirkt auch nach dem Kauf noch nach (Kotler et al., 2003). Es muss nicht immer sein, dass alle fünf Stufen bei einer Entscheidungsfindung durchlaufen werden. Einzelne Stufen können übersprungen oder in einer anderen Reihenfolge durchlaufen werden. Oder die einzelnen Prozessschritte können unterschiedlich intensiv ausfallen, je nachdem, ob es sich um ein Produkt mit hohem oder niedrigem Engagement (low oder high involvement) handelt (Mittal, 1989; Kotler et al., 2003). Die Entscheidungsfindung ist kein statisches Konstrukt, sondern ein dynamischer Prozess mit Wechselwirkungen. Der Kunde steht dem Entscheidungsfindungsprozess beispielsweise anders gegenüber, wenn er ihn regelmässig durchläuft, als wenn er sich zum ersten Mal damit auseinandersetzt. Besonders bei der

[12] Kotler (1972) definiert eine Transaktion als: "The exchange of values between two parties" (S. 48). Die Interaktion wird definiert als eine Wechselwirkung, in der „sich Individuen oder Gruppen durch ihr aufeinander bezogenes Handeln gegenseitig beeinflussen" (Reinhold, 1997, S. 305). Die umfassende Definition von Kotler (1972) beinhaltet sowohl tangible als auch intangible Güter, schliesst also die Interaktion mit ein, da unter Werten auch immaterielle Werte verstanden werden. In dieser Arbeit wird deshalb bei der Verwendung des Begriffs Transaktion die Interaktion automatisch impliziert.

Entscheidungsfindung im Online-Umfeld kommen weitere Faktoren hinzu, welche für Unternehmen und Kunde zu beachten sind.

Speziell bei der Entscheidungsfindung im Online-Umfeld ist, dass zwischen dem Entscheid bei materiellen Produkten eine Zeitdivergenz besteht. Man entscheidet sich, zahlt im Voraus und wartet darauf, dass das Produkt geliefert wird. Online-Geschäftsmodell-Anbieter sollten ihre Nutzer idealerweise bei jeder Phase des Entscheidungsfindungsprozesses unterstützen (Kroeber-Riel, 1996). Darley et al. (2010) erweiterten das EKB-Modell (Engel, et al., 1978; 1986) und adaptierten es für die Erforschung des Online-Konsumentenverhalten. Das modifizierte Modell von Darley et al. (2010) ist so umfassend, dass es die Wechselwirkungen, Moderatoren und Gegebenheiten des neuen Internets voll integrieren kann. Das erweiterte Modell erkennt die zentrale Rolle der fünf Phasen des Entscheidungsfindungsprozesses an, schliesst aber Wechselwirkungen und externe Einflussfaktoren mit ein und spezifiziert die Bewertung der Alternativen, wie in Abbildung 12 dargestellt wird.

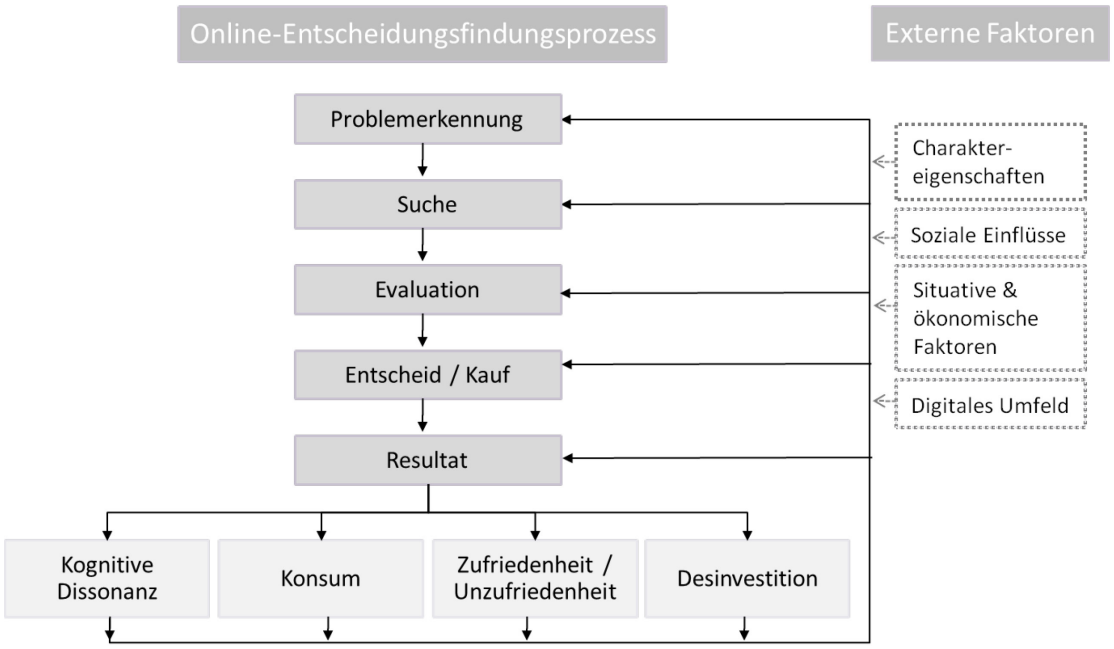


Abbildung 12: Der Online-Entscheidungsfindungsprozess (eigene Darstellung in Anlehnung an Darley et al., 2010)

Die Autoren erwähnen explizit, dass die Informationssuche in eine interne (Erfahrung) und eine externe Suche (persönliche, kommerzielle und öffentliche Informationsquellen) eingeteilt wird. Des Weiteren spezifiziert das Modell von Darley et al. (2010) die Bewertung von Alternativen. Die Autoren gehen davon aus, dass die Bewertung von Alternativen von der individuellen Überzeugung, Haltung und Einstel-

lung sowie von den Absichten der jeweiligen Person abhängig ist. Des Weiteren werden die Transaktion und die Folgen der Entscheidung differenziert in unterschiedliche Wahrnehmungen (kognitive Dissonanz), den Konsum des Produktes oder der Dienstleistung, die Zufriedenheit oder Unzufriedenheit sowie in die Desinvestition. Diese Entscheidungsfolgen haben einen Einfluss darauf, wie der Nutzer bei der nächsten Online-Entscheidung in den Prozess einsteigen wird. Neben den oben erwähnten Einflussfaktoren spielen auch im Online-Umfeld externe Faktoren für die Entscheidungsfindung eine wichtige Rolle. Diese externeren Faktoren (auch Umweltfaktoren genannt) werden in vier Gruppen eingeteilt: (1) Persönlichkeitsmerkmale: Motive, Werte, Lebensstil und Persönlichkeit; (2) soziokulturelle Faktoren: Kultur, Referenzgruppe, Familie; (3) situative und ökonomische Faktoren; (4) Online-Umgebung: Qualität der Webseite, Schnittstellen zur Webseite, Zufriedenheit und Erfahrung mit der Webseite.

Wenn ein Kunde das erste Mal eine Transaktion mit einem Geschäftsmodell-Anbieter tätigt, wird von einem Erstkauf (initial purchase) gesprochen. Hat der Kunde den Entscheidungsfindungsprozess durchlaufen und ist er mit seinem Entscheid zufrieden, wird er eventuell wieder bei dem Anbieter eine Transaktion tätigen (repeated purchase) (Blackwell et al., 2001: Solomon, 2004). Vertrauen wird als zentraler Faktor im gesamten Entscheidungsfindungsprozess im Internet betrachtet und beeinflusst die zukünftigen Verhaltensabsichten (Yoon, 2002; Ha & Perks, 2005; Cho, 2006; Jiang, Jones & Javie, 2008; Darley et al., 2010).

2.1.4 Zusammenfassung

Nutzer verbringen heute immer mehr Zeit im Internet – die Arbeitswelt beruht zunehmend auf einer Vielzahl von Online-Geschäftsmodellen und auch die Kommunikation in der Freizeit findet verstärkt im Web statt. Besonders durch mobile Endgeräte wie Tablets oder Smartphones wird das Internet allgegenwärtig. Immer mehr Unternehmen stellen Applikationen zur Verfügung, damit Nutzer sich untereinander verbinden, austauschen und miteinander kooperieren können (Afuah & Tucci, 2001; Mahadevan, 2000; O'Donnell, 2002; Rust et al., 2002). Im B2C- und B2B-Bereich stehen vier Geschäftsmodelle im Fokus dieser Dissertation: Online-Information, Online-Shopping, Online-Banking und soziale Netzwerke. Voraussetzung für alle Geschäftsmodelle im Internet ist die Bereitschaft der Nutzer, persönliche Daten zur Verfügung zu stellen. Persönliche Daten sind im Internet wie eine Währung zu verstehen, die im Rahmen einer Transaktion getauscht und gehandelt wird. Besonders bei personalisierten Geschäftsmodellen sind persönliche Daten als kritischer Erfolgsfaktor zu betrachten. Der Nutzer wägt bei jeder Transaktion ab, ob er die geforderten Daten gegen den versprochenen Nutzen eintauschen möchte. Die mediale Präsenz von Datenschutzskandalen löst Bedenken bezüglich der Datensicherheit und des Datenschutzes aus. Wie sich der Nutzer im Internet bei einer Transaktion entscheidet, ist Gegenstand der Marktforschung. Der Entscheidungsvorgang beim Käufer wird in fünf grundlegende Stufen eingeteilt: Problemerkenntnis, Informationssuche, Bewertung von Alternativen, Auswahl und Kaufentscheid sowie Entscheidungsfolgen. Im digitalen Umfeld spielen die Qualität der Website, Schnittstellenkompatibilität, technische Stabilität und Erfahrungen mit dem Internet eine entscheidende Rolle. Das Kaufverhalten ist das Ergebnis unterschiedlichster Faktoren wie zum Beispiel kultureller, sozialer, persönlicher oder psychologischer Einflüsse (Kotler et al., 2003). Mit dem Wissen über das Verhalten ihrer Kunden und Konsumenten sind Unternehmen eher in der Lage, ein effizientes Marketing- und Kommunikationsprogramm zu lancieren.

Dieses Kapitel hat gezeigt, wie wichtig persönliche Daten für Online-Anbieter sind und dass der Handel mit persönlichen Daten zum lukrativen Geschäftsmodell geworden ist. Dies rückt Fragen in Bezug auf Privacy und Sicherheit der Daten im Netz in den Mittelpunkt der gesellschaftlichen Debatte. Deshalb widmet sich das nächste Kapitel der Literaturübersicht zum Thema Privacy.

2.2 Das Problem: Privacybedenken und der Wunsch nach Kontrolle

Im vorhergehenden Kapitel 2.1.2 wurden zwei massgebliche Treiber und Hürden für Online-Geschäftsmodelle identifiziert: die Privacy und die Sicherheit der Nutzer. Noch nie war es so einfach, unser Leben und unsere Gewohnheiten zu beobachten, zu dokumentieren, abzuspeichern und auszuwerten. Doch diese Vorteile bergen auch verschiedene Risiken, denn die Daten können gesammelt, aggregiert und dann verkauft werden (Cai & Gantz, 2000; Montgomery & Pasnik, 1996; Moscardelli & Liston-Heyes, 2004; Youn, 2009). Urban et al. (2009) stellen fest: "Privacy and security have become the new baseline from which one evaluates an online merchant's trustworthiness." Deshalb widmet sich das folgende Kapitel 2.2.1 der Entstehungsgeschichte und dem Bedürfnis eines Individuums nach Privacy. Die Bedeutung von Privacy im Internetzeitalter wird im Kapitel 2.2.2 vertieft und anschliessend wird im Kapitel 2.2.3 auf die Einflussfaktoren von Privacybedenken und auf die Strategien zum Schutz der Privacy eingegangen. Im Schlusskapitel 2.2.4 werden die Erkenntnisse zum Thema Privacy zusammengefasst.

2.2.1 Entstehungsgeschichte und Definition von Privacy

Lanier und Saini (2008) vergleichen in ihrer Literaturübersicht Privacy mit dem menschlichen Bedürfnis nach Teilnahme: Während sich Menschen als soziale Wesen in der Regel die Interaktion mit anderen Menschen wünschen, haben sie auch das Bedürfnis nach Rückzug, Autonomie und Selbstkontrolle. Westin (1967) beschreibt diese Divergenz folgendermassen: "Either too much or too little privacy can create imbalances which seriously jeopardize the individual's well-being" (S. 40). Das Bedürfnis nach Privacy bildet sich hauptsächlich aus dem individuellen Wunsch, den Fluss der persönlichen Daten und Informationen kontrollieren zu können sowie die öffentliche Verfügbarkeit dieser Daten einzuschränken. Privacy ist somit kein absolutes Konstrukt, sondern ein subjektiver Balanceakt zwischen Freigabe und Kontrolle. Im folgenden Kapitel 2.2.1.1 wird kurz auf die Entstehungsgeschichte der Privacy-Diskussion eingegangen, die unterschiedlichen Definitionen von Privacy werden im Kapitel 2.2.1.2 und Konsumenten-Privacy im Kapitel 2.2.1.3 behandelt.

2.2.1.1 Der erste Meilenstein: „The Right to Privacy“

Für ein tiefer gehendes Verständnis von Privacy wird im Folgenden kurz auf deren Entstehungsgeschichte eingegangen:

Die ersten Regelungen bezüglich der Privacy des Individuums entstanden zu Beginn des 19. Jahrhunderts. Gründe dafür lagen im technischen Fortschritt, insbesondere im Aufkommen der Massenmedien (Penny-Press um 1850) sowie der Handkamera für die Amateurfotografie (1870) (Warren & Brandeis, 1890). Nun wurden zum ersten Mal Bilder von Privatpersonen auch ohne deren Einwilligung aufgenommen, vervielfältigt und veröffentlicht. Der Richter Lois Brandeis und der Schriftsteller und Rechtsanwalt Samuel Warren nahmen sich des Themas an und veröffentlichten im Jahr 1890 das wegweisende Schriftstück „The Right to Privacy“, in dem erste Überlegungen zum Schutz der Privacy und dem Datenschutz abgehandelt werden (Warren & Brandeis, 1890). Ihre Argumente lauteten: “Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual […]. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life […]” (o. S.). Darin definieren sie Privacy als “The right to be let alone” (o. S.). Ziel der Schrift war es, die Privacy von Individuen vor ungewollten Veröffentlichungen zu schützen. Die Kernaussage der Schrift ist, dass jedes Individuum das Recht haben sollte, selber entscheiden zu können, welche Informationen wann veröffentlicht werden. Ausgeschlossen sind jedoch Informationen von öffentlichem Interesse: “The right to privacy does not prohibit any publication of matter which is of general interest.” (o. S.). Das Recht auf Privacy endet bei Veröffentlichung der Information durch das Individuum oder durch deren Einwilligung zur Veröffentlichung: “The right to privacy ceases upon the publication of the facts by the individual, or with his consent.” (o. S.).

Im nächsten Kapitel werden der wissenschaftliche Diskurs und die Definition von Privacy besprochen.

2.2.1.2 Literaturübersicht und Diskussion des Konstrukts Privacy

Bevor ins Thema Privacy eingestiegen werden kann, muss klar definiert werden, was unter Privacy verstanden wird. In der Privacy-Literatur wird oft zwischen dem Konzept der Privacy sowie dem Recht auf Privacy unterschieden (Marwick, Diaz & Palfrey, 2010; Solove & Schwartz, 2009). Der Rechtswissenschaftler Prosser (1960) verstand Rechtsverletzungen im Bereich der Privacy nicht als ein einheitliches, unitäres Konzept. Deshalb sammelte er umfangreiches Fallmaterial und versuchte, dieses zu analysieren und die unterschiedlichen Verletzungen der Privacy abzugrenzen und zu systematisieren (Lanier & Saini, 2008). Er unterschied vier Deliktbereiche: (1) Verletzung der Intimsphäre oder privater Angelegenheiten; (2) Verwendung von privaten Tatsachen; (3) Bekanntgabe und Offenlegung von privaten Daten sowie (4) eine Person absichtlich im falschen Licht zeigen. Prossers (1960) zusammenfassende Analyse der Verletzung der Privacy hatte besonderen Einfluss auf die amerikanische Rechtsprechung und bestimmt noch heute das Verständnis von Privacy, besonders im amerikanischen Privatrecht (Amelung, 2002, S. 67). Verschiedene Autoren kritisieren, dass diese vier Deliktstypen weder trennungsscharf noch abschliessend sind (Amelung, 2002; Nowak & Phelps, 1997; Lanier & Saini, 2008; Foxman & Kilcoyne, 1993). Zum Beispiel schliesst „jemanden absichtlich im falschen Licht zeigen“ eine Weitergabe von persönlichen Daten für den kommerziellen Gebrauch nicht mit ein, da die Daten erstens auf Tatsachen beruhen und zweitens nicht veröffentlicht werden.

Aufgrund dieser Limitationen argumentierten verschiedene Rechtswissenschaftler, dass das Konzept der Privacy als Ganzes betrachtet werden sollte und nicht als ein mehrdimensionales Konstrukt, wie dies von Prosser vorgeschlagen worden war (Benn, 1971; Bloustein, 1964; Gavison, 1980; Graham, 1987). Sie argumentierten, dass Privacy als Schutz der Menschenwürde betrachtet werden sollte (Bloustein, 1964; Gavison, 1980). Diese einheitliche Sichtweise auf Privacy basiert auf der Einstellung, dass jeder Mensch selber über seine persönlichen Daten bestimmen sollte (Lanier & Saini, 2008). Aus dieser konsolidierten Sichtweise heraus entstanden unterschiedliche Definitionen von Privacy. Westin (1967) definiert Privacy als: "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small group intimacy, or, when among larger

groups, in a condition of anonymity or reserve" (S. 6 f.). Westin (1967) argumentiert, dass die Privacy aus vier Kernelementen besteht: Alleinsein, Intimität, Anonymität und Zurückhaltung. Alleinsein bedeutet, physisch von anderen getrennt zu sein und nicht unter Beobachtung zu stehen. Intimität ist der Zustand, sich in einer kleinen, überschaubaren Einheit zu befinden, wie dies zum Beispiel die Familie ist, während Drittpersonen von Ausserhalb der Zugang zur Einheit verwehrt bleibt. Anonymität ist, wenn man sich zwar in der Öffentlichkeit befindet, nicht aber identifizierbar ist und auch nicht beobachtet wird. Zurückhaltung bedeutet, dass eine Person psychologische Barrieren aufbaut, um sich selbst vor ungewollten Eingriffen zu schützen. Diese Definition fokussiert darauf, selbst über seine persönlichen Daten und den Zugriff auf diese bestimmen zu können.

Dieser Fokus auf die Kontrolle der eigenen Daten zeigt sich auch in den Definitionen von Jourard (1966), Fried (1968), Parker (1974) oder bei Belanger, Hiller und Smith (2002), die Privacy als die Möglichkeit definieren, Informationen über sich selbst zu kontrollieren. Die Definition von van Den Haag (1971) hingegen rückt vermehrt den sozialen Aspekt von Kontrolle und Zugang zu persönlichen Daten ins Zentrum: “Privacy is the exclusive access of a person to a realm of his own. The right to privacy entitles one to exclude others from (a) watching, (b) utilizing, and (c) invading his private realm.” (S. 149). Allgemeiner halten sich Rust et al. (2002), die Privacy definieren als “the degree to which personal information is not known by others” (S. 456). Lessig (2002) und Garfinkel (2000) hingegen verstehen Privacy als Eigentum und als ein handelbares Gut, das einen Markt und einen Preis hat. Diese Auffassung von Privacy geht einher mit der Kosten-Nutzen-Überlegung bei der Veröffentlichung privater Daten (siehe auch Kapitel 2.1.2.1). Privacy kann als Gut betrachtet werden, jedoch kein exklusives, denn man kann Privacy anderen zugestehen, ohne dadurch selbst weniger Privacy zu besitzen. Auch Informationen können viele Personen gleichzeitig nutzen, ohne dass dabei anderen etwas entzogen werden würde. Informationelle Privacy bedeutet, die Kontrolle über den Fluss der Information über die eigene Person zu besitzen. „Unter diesem Blickwinkel sind Informationen und Privacy komplementär, denn der Umlauf von mehr persönlichen Informationen in den Händen einer Gesellschaft bedeutet weniger Privacy für die Mitglieder dieser Gesellschaft; der geringere Umlauf persönlicher Informationen bedeutet grössere Privacy“ (Drüeke & Weber, 2007, S. 30).

Die Philosophin Rössler (2001) unterscheidet, ähnlich wie Solove (2002; 2005), drei Dimensionen von Privacy[13]: (1) dezisionale, (2) informationelle und (3) lokale Privacy. (1) Dezisionale Privacy räumt jedem ein „Recht auf die Bestimmung seines eigenen Lebens" (Rössler, 2001, S. 30) ein. Entsprechend kann eine Person ihre Entscheidungen, Handlungen, Verhaltens- und Lebensweisen – sofern diese im privaten sozialen Raum stattfinden – selbst bestimmen und wählen, ohne dass Drittpersonen dabei einen Anspruch auf Bewertungen, Einspruch oder Urteil haben (Drüeke & Weber, 2007). Bei der Frage nach der (2) informationellen Privacy geht es um die Kontrolle über den Fluss der Information über die eigene Person oder, wie es Rössler (2001) ausdrückt: „Wer was wie über eine Person weiss" (S. 20). Bei der informationellen Privacy geht es darum, selbst zu entscheiden, welche persönlichen Informationen an wen weitergegeben werden. Diese Dimension setzt demnach die Kontrolle des Informationsflusses über die eigene Person voraus (Drüeke & Weber, 2007). Die dritte Dimension umfasst die (3) lokale Privacy. Diese beinhaltet die Gewährleistung des Schutzes intimer Beziehungen und Rückzugsmöglichkeiten in der privaten Wohnung (Rössler, 2001).

Im nächsten Kapitel wird insbesondere auf die Privacy von Konsumenten und Nutzern eingegangen.

2.2.1.3 Die Privacy von Konsumenten und Nutzern

Der Grossteil der Definitionen von Consumer Privacy orientiert sich an der Definition von Privacy von Warren und Brandeis (1980), in der Privacy als "the right to be let alone" bezeichnet wird (o. S.). Goodwin (1991) definiert Consumer Privacy als "the consumer's ability to control (a) presence of other people in the environment during a market transaction or consumption behavior and (b) dissemination of information related to or provided during such transactions or behaviors to those who were not present" (S. 152). Der erste Teil dieser Definition beinhaltet die sozialen Aspekte von Privacy, denn sie verweist auf die Möglichkeit des Konsumenten, über die Präsenz von Drittpersonen bei einer Transaktion entscheiden zu können. Dies betrifft

[13] Solove (2002) unterteilt Privacy in sechs Unterpunkte: (1) das Recht, allein gelassen zu werden, (2) die Möglichkeit, sich vor ungewolltem Zugriff von Drittpersonen zu schützen, (3) Geheimhaltung, (4) Kontrolle über persönliche Informationen, (5) Persönlichkeit (6) sowie Intimität (S. 1099 ff.).

insbesondere die Anbieterseite, nicht aber die Präsenz von anderen Konsumenten (Milne & Gordon, 1993; Lanier & Saini, 2008). Der zweite Teil der Definition bezieht sich auf die Möglichkeit, selbst bestimmen zu können, welche Informationen wem zur Verfügung gestellt werden, insbesondere im Hinblick auf die Datenweitergabe von Marketingfirmen (Jones, 1991; Lanier & Saini, 2008). Basierend auf diesen beiden Arten der Kontrolle, der Sozialkontrolle und der Informationskontrolle, können nun vier Stufen der Privacy definiert werden: (1) die totale Kontrolle, (2) Kontrolle über die Umwelt, in der der Austausch der Information stattfindet, (3) Kontrolle über den Gebrauch und die Veröffentlichung der privaten Informationen sowie (4) keine Kontrolle, wie in Abbildung 13 dargestellt (Goodwin, 1991).

Abbildung 13: Privacystufen (eigene Darstellung in Anlehnung an Goodwin, 1991)

Die totale Kontrolle hat ein Konsument dann, wenn er einerseits Kontrolle über die Umwelt und andererseits Kontrolle über die Veröffentlichung der jeweiligen Information besitzt. Diese Situation ist die höchstmögliche Stufe von Privacy. Die Kontrolle über die Umwelt, in der der Austausch der Information stattfindet, bedeutet, dass Konsumenten über die Präsenz von Drittpersonen bestimmen können, nicht aber Kontrolle über den Gebrauch ihrer privaten Informationen haben. Haben Kunden Kontrolle über den Gebrauch und die Veröffentlichung der privaten Informationen, ist es dennoch möglich, dass sie keine Kontrolle über die Umwelt besitzen. Die letzte Stufe bedeutet, gar keine Kontrolle über die Privacy seiner Daten zu besitzen. Dies beinhaltet sowohl fehlende Kontrolle über die Umwelt, in der der Austausch der Informationen stattfindet, als auch fehlende Kontrolle über die Veröffentlichung der jeweiligen Information (Goodwin, 1991).

Die von Goodwin (1991) vorgeschlagene, auf Kontrolle basierende Definition von Consumer Privacy wird von verschiedenen Autoren durch die Dimension Verbraucherbildung ergänzt (Nowak & Phelps, 1997; Culnan, 1995; Foxman & Kilcoyne, 1993). Die Dimension der Bildung bedeutet nicht nur, dass Konsumenten vollständig informiert sind über die Informationspraktiken der Unternehmen und über die geltenden Privacy-Rechte für die jeweilige Transaktion, sondern auch, dass Konsumenten diese verstehen (Foxman & Kilcoyne, 1993). Dies bedeutet, dass Konsumenten

wissen müssen, welche Informationen über sie gesammelt, wie und weshalb diese gesammelt werden (Belanger & Hiller, 2006). Sie müssen nachvollziehen können, wie diese Daten weiterverwendet werden, besonders wenn die Verwendung über den ursprünglichen Verwendungszweck hinausgeht. Ausserdem müssen sie ihre Rechte in Bezug auf die Sammlung, Aggregation und Weiterverwendung ihrer privaten Daten kennen und durchsetzen können.

Das Aufkommen einer neuen Generation von Kommunikationstechnologien und die massive Ausweitung der Medienlandschaft rückt Privacy-Fragestellungen immer mehr ins Zentrum des gesellschaftlichen Interesses und offenbart neue politische, rechtliche und wirtschaftliche Herausforderungen. Deshalb wird die Bedeutung von Privacy im Internetzeitalter im nächsten Kapitel näher betrachtet.

2.2.2 Bedeutung von Privacy im Internetzeitalter

Technologische Errungenschaften veranlassen uns auch heute, 120 Jahre nach den Überlegungen von Warren und Brandeis (1890), das Verständnis von Privacy zu überdenken. Damals argumentierten die Autoren, dass das Konzept der Privacy durch gesellschaftlichen und wirtschaftlichen Wandel modifiziert und angepasst werden müsse. Diese Überlegungen besitzen nach wie vor ihre volle Gültigkeit. Durch die stetige Weiterentwicklung der Massenmedien stehen wir vor ähnlichen Fragen wie im neunzehnten Jahrhundert. Dass persönliche Informationen für die ganze Netzwelt einsehbar sind, ist zum Alltag der Informationsgesellschaft geworden. Scott McNealy, der ehemalige CEO des Computerherstellers Sun Microsystems, sagte bereits um die Jahrtausendwende: “You have zero Privacy anyway. Get over it” (Sprenger, 1999). Auch Mark Zuckerberg, der CEO und Mitgründer der Social Networking Site Facebook, sagte in einem Interview, dass das Zeitalter von Privacy vorbei ist und sie nicht mehr zur sozialen Norm gehört (Arrington, 2010). Das Internet hat die Art und Weise, wie Informationen, Wissen und Unterhaltung kreiert, konsumiert, weiterverarbeitet und verbreitet wird, fundamental verändert (Gasser et al., 2011). Privacy verliert jedoch nicht an Relevanz, im Gegenteil, sie wird durch die sich verändernden Medien neu definiert und gewinnt durch die Möglichkeiten der Offenlegung und Vernetzung an Bedeutung. Die folgenden Kapitel befassen sich mit der Veränderung von Privacy durch das Internet (2.2.2.1) und mit den Bedenken der Internetnutzer in Bezug auf ihre Privacy (2.2.2.2).

2.2.2.1 Veränderung von Privacy durch das Internet

George Orwell (1948) schreibt in seinem Roman „1984“ von der Schreckensgestalt „Big Brother“. Heute gibt es vielleicht nicht den Überwachungsstaat wie im Roman, dafür aber viele kleine Big Brothers. Heute werden wir von vielen grossen Brüdern und Schwestern gleichzeitig, weltweit und in Echtzeit überwacht. Mittlerweile haben wir uns daran gewöhnt, dass wir auf Schritt und Tritt von Kameras überwacht werden, trotzdem sind wir uns des Ausmasses der Überwachung häufig nicht bewusst.

So weiss beispielsweise kaum jemand, dass wir über unser Mobiltelefon metergenau geortet werden können und dass so ganze Bewegungsprofile von uns erstellt werden können, wie dies die Locationgate-Affäre von Apple[14] eindrücklich aufzeigt (Schmundt, 2011). Die Miniaturisierung sowie die günstige Verfügbarkeit von Audio- und Videotechnik machen es möglich, dass jedermann überwachen, aufnehmen, abspeichern und veröffentlichen kann, was er sieht und hört, ohne dass dies bemerkt wird. Mittels geeigneter Software können jeder Tastaturschlag und jede Mausbewegung im Netz registriert und in einem digitalen Dossier gespeichert werden. Die Furcht vor einem Big Brother wurde so durch die Angst vor zahlreichen Big Brothers ersetzt.

Wir verbringen einen grossen Teil unseres Lebens in der Öffentlichkeit, real und immer häufiger auch virtuell auf Internetangeboten wie Facebook, Flickr oder YouTube. Um an Online-Transaktionen teilnehmen zu können und um massgeschneiderte Produkte und Dienstleistungen erhalten zu können, müssen Kunden persönliche Daten und Präferenzen zur Verfügung stellen (siehe auch Kapitel 2.1.2.1). Sobald Internetnutzer persönliche Informationen ins Netz stellen, werden diese öffentlich zugänglich gemacht, sie sind ab diesem Zeitpunkt möglicherweise bereits über

[14] Alasdair Allan stiess auf seinem iPhone auf eine ihm unbekannte Datei „consolidated.db“ und schrieb ein Programm, um die Daten sichtbar zu machen. Nun konnte er aus der Vogelperspektive alle Ortsdaten sehen: 28’000 Ortsdaten hatte das Gerät gespeichert mit einer Genauigkeit von unter einem Kilometer und sekundengenauem Zeitstempel. Er fand heraus, dass die Firma Apple ohne sein Wissen oder seine Zustimmung 293 Tage lang heimlich seine Bewegungen im iPhone abspeicherte. Das Bewegungsprofil betraf Millionen Besitzer von iPhones und iPads weltweit und die Publikmachung der heimlichen Speicherung löste einen Skandal aus. Die Affäre bekam den Spitznahmen „Locationgate“, in Anspielung an den Watergate-Skandal (Schmundt, 2011). Der Konzern spricht von einem Versehen, Datenschützer und Nutzer zeigen sich aber alarmiert und befürchten, dass Apple die Bewegungsprofile zu Geld machen will (Schmundt, 2011).

Suchmaschinen auffindbar und zwar permanent oder „für immer“, wie es Giffen (2008) ausdrückt. Die Nutzung des Internets geht also immer einher mit einem gewissen Verlust von Privacy (Rust et al., 2009).

Heutige Internetnutzer, insbesondere Digital Natives[15], haben bezüglich ihrer persönlichen Daten eine sehr unterschiedliche Handhabung. Einerseits laden sie haufenweise persönliche Daten ins Netz und führen ihre Konversationen öffentlich (Hoffmann & von Kaenel, 2010a; Christofides et al., 2009). Mark Zuckerberg äusserte hierzu: “People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time” (Arrington, 2010). Palfrey und Gasser (2008) vergleichen die Datenspur der Digital Natives mit einem Tattoo, das eine Person das ganze Leben begleitet und das man fast nicht mehr los wird. Einige Autoren gehen sogar so weit zu sagen, dass Jugendliche nicht auf ihre Privacy achten (Kornblum, 2007; Nussbaum, 2007; Moscardelli & Liston-Heyes, 2004). Andererseits sind Nutzer erstaunt, wenn Drittparteien, zum Beispiel Eltern, Lehrer oder Marketingfirmen, mitlesen und diese Daten sammeln. Es kann beobachtet werden, dass Bedenken bezüglich der Privacy der Internetnutzer wie auch die mediale Präsenz aufgrund von Verfehlungen vieler Firmen stetig zunehmen (Okazaki, Li & Hirose, 2009), wie der gi-

[15] Palfrey und Gasser (2008) unterteilen die Internetnutzer in Digital Natives und Digital Immigrants. Digital Natives sind nach 1980 geboren, haben Zugang zu digitalen Technologien und haben die Fähigkeiten, diese zu nutzen. Die Immigrants hingegen sind nicht mit den digitalen Technologien aufgewachsen und müssen die Fähigkeiten, diese zu nutzen, erst erlernen.

gantische Datendiebstahl von Sony Playstation[16] oder der tragische Erpressungsversuch bei SchülerVZ[17] zeigen.

Der Verlust von Teilen der Privacy ist eine der Herausforderungen, die es bei der Verwendung digitaler Geschäftsmodelle zu bewältigen gilt (Hoffman et al., 1999a; Luo, 2002; Udo, 2001). Einen Eingriff in die Privacy umschreibt Luo (2002) im Kontext des Internets folgendermassen: "In the arena of Internet marketing, invasion of privacy is commonly interpreted as the unauthorized collection, disclosure, or other use of personal information such as selling it to other e-marketers" (S. 112). Laut Richards (1997) war kein anderes Medium ein solcher Katalysator für Eingriffe in die Privacy wie das Internet.

Bis vor der Etablierung sozialer Medien herrschte eine klare Trennung zwischen der öffentlichen und der privaten Sphäre. Besonders für Digital Natives, aber immer mehr auch für „Digital Immigrants" verschwimmt diese Trennung zusehends (Marwick et al., 2010; Prensky, 2001; Taraszow et al., 2010). Palfrey und Gasser (2008) schreiben: "Privacy might be a problem for anyone who leads a life mediated in part by digital technologies" (S. 61 f.). Der Journalist und Autor Christopher Harper (1998) vertritt den Standpunkt, dass Internetnutzer ihre Privacy nur schützen könnten, indem sie alle Endgeräte abschalteten. Durch das Internet und insbesondere

[16] Sony Playstation erlebte einen der grössten Datendiebstähle der Geschichte: Hacker brachen im April 2011 in das Netzwerk von Sony Playstation und dem Video- und Musikservice Qriocity ein und stahlen Adressen, Passwörter und eventuell Kreditkartennummern von über 77 Millionen Nutzern (Schmundt, 2011). Der japanische Unterhaltungselektroriese stoppte daraufhin das Angebot, informierte seine Kunden aber erst eine Woche später über die Hacker-Attacken (Kremp, 2011). Die Demütigung für Sony ging aber weiter. Im Frühjahr 2011 kam es noch zu mehreren Hacker-Angriffen auf den Grosskonzern und dessen Tochterfirmen. Zum Beispiel verschafften sich Hacker Zugang zu SonyPictures.com und somit wiederum zu Millionen von Nutzerdaten (Witte & Reissmann, 2011). Tausende der gestohlenen Kundendaten waren vorübergehend im Internet für jedermann einsehbar (Kremp, 2011). Der Börsenwert von Sony brach danach um über zwei Milliarden Euro ein (Schmundt, 2011).

[17] Ende 2009 wurde bekannt, dass aus dem sozialen Netzwerk „SchülerVZ" eine Million Datensätze mit persönlichen Profilen kopiert worden waren. Zu den kopierten Daten zählten Angaben zu Schule, Namen, Geschlecht und Alter der Nutzer sowie Profilfotos. Die Betreiber des Netzwerks wurden daraufhin von einem Unbekannten kontaktiert, der 80'000 Euro für die Rückgabe der Datensätze forderte. Das Unternehmen wandte sich an die zuständigen Behörden und diese verhaftete daraufhin einen polizeibekannten 20-Jährigen. Der Schüler nahm sich daraufhin in seiner Zelle das Leben (Augsburger Allgemeine, 2009; Greif, 2009; Spiegel Online, 2010; Seidler, 2009).

durch die Sozialen Medien gewinnt die digitale Privacy immer mehr an Bedeutung. Im nachfolgenden Kapitel werden deshalb die Privacybedenken der Nutzer im Internetkontext vertieft betrachtet.

2.2.2.2 Privacybedenken im Internetkontext

Ein möglicher Verlust von Privacy gehört zu den Hauptsorgen der Internetnutzer (Hoffman et al., 1999b; Luo, 2002; Udo, 2001; Smith, Milberg & Burke, 1996). Bedenken über Privacy im Internet bezieht sich auch auf die Unsicherheit, was mit den im Internet eingegebenen Daten geschieht (Dinev & Hart, 2005; 2006). Seit das Internet in den 1990er-Jahren populär wurde, ist die digitale Privacy Gegenstand von Diskussionen und Untersuchungen (Smith et al., 1996; Chellappa & Sin, 2005; Marwick et al., 2010). Forscher in den Bereichen Informationssysteme und Marketing argumentieren, dass Privacy und Verbraucherbedenken einer der Kernpunkte in der technologiebasierten Umgebung sind (Miyazaki & Fernandez, 2000; Chellappa & Sin, 2005; Stewart & Segars, 2002).

Die Angst um die persönlichen Daten ist kein Phänomen des 21. Jahrhunderts. In ihrer Studie von 1985 über Privacy im Internet konnten Vidmar und Flathery aufzeigen, dass die untersuchten Probanden das Gefühl hatten, dass Unternehmen im Internet mehr Daten sammeln, als eigentlich notwendig wäre. Die Probanden waren der Ansicht, dass die gesammelten und aggregierten Informationen nur selten ausschliesslich für den Zweck genutzt werden, für den sie ursprünglich gesammelt wurden (Vidmar & Flathery, 1985). Im Onlinebereich sind Konsumenten nicht nur über die Privacy ihrer Daten besorgt, welche Rückschlüsse auf ihre Identität ermöglichen, sondern auch über breitere Datenspeicherungen, welche zu einem späteren Zeitpunkt aggregiert werden könnten (Chellappa & Sin, 2005). Helene Nissenbaum (2009) unterteilt die Anliegen der Nutzer bezüglich Privacy in neuen Technologien in die drei Kategorien (1) Monitoring und Tracking, (2) Verbreitung und Veröffentlichung sowie in (3) Aggregation und Analyse (Abbildung 14).

Monitoring & Tracking	Identifikation, Überwachung, kommerzielle Nutzung
Verbreitung & Veröffentlichung	Weitergabe an Dritte, Kontaktierung, Herauslösung Kontext, Shaming
Aggregation & Analyse	Digitale Dossiers, Identitätsdiebstahl

Abbildung 14: Zentrale Privacybedenken (eigene Darstellung in Anlehnung an Nissenbaum, 2009)

Diesen drei Kategorien werden zur besseren Illustration einige konkrete Bedenken der Nutzer zugeteilt; die Auflistung ist nicht abschliessend:

(1) Monitoring und Tracking

Identifikation: Wie weit die technischen Möglichkeiten fortgeschritten sind, um Nutzer zu identifizieren, zeigen die Einsätze biometrischer Erkennungstechniken wie Augenscan oder Fingerabdruckscan für Zugangskontrollen, aber auch die Gesichtserkennungsfunktion in sozialen Netzwerken (Stratenschulte, 2011).

Überwachung: Öffentliche Stellen wie auch Privatpersonen können durch RFID[18]-Tags, Gesichtserkennungssysteme, Tracking-Cookies oder Marketingmassnahmen Verhaltensmuster der Nutzer, Kunden oder Bürger erstellen (Ström, 2006; Nissenbaum, 2009). Zum Schutz von Kindern haben Eltern oder Lehrer oft das Bedürfnis, deren Aktivitäten, insbesondere im Internet, zu überwachen und zu kontrollieren, um im Ernstfall eingreifen zu können. Dies kann dazu führen, dass Kinder oder junge Erwachsene keinen Raum mehr haben, in dem sie ihre Identität erkunden und entwickeln können (Boyd, 2007).

Kommerzielle Nutzung: Unternehmen pflegen umfangreiche Datenbanken, welche Informationen über das Verhalten ihrer Kunden und Nutzer beinhalten. Automatisierte Analyseinstrumente wie Cookies oder Clickstream Monitoring lassen diese Datenbanken beständig anwachsen (Rust et al., 2002; Olivero & Lunt, 2004). Diese gesammelten Daten können für kommerzielle Zwecke ge- oder missbraucht werden und an Drittpersonen weiterverkauft werden (Montgomery & Pasnik, 1996).

[18] RFID = radio-frequency identification was als Identifizierung mit Hilfe elektromagnetischer Wellen übersetzt werden kann.

(2) Verbreitung und Veröffentlichung

Weitergabe der Daten an Dritte: Durch die Ausbreitung digitaler Technologien ist es so einfach wie nie zuvor, persönliche Daten herunterzuladen. Einmal digitalisiert, sind diese Daten für immer im Netzuniversum auffindbar und können für kommerzielle Zwecke, von Krankenkassen, Finanzbehörden oder Versicherungen gekauft werden (Mills, 2008). Diese Daten können schneller und einfacher denn je weitergeleitet, veröffentlicht und gehandelt werden. Kunden und Nutzer sind besorgt, dass ihre Daten und Kundenprofile an unbekannte Drittpersonen weitergeleitet und dass aus den vielen einzelnen Daten digitale Dossiers erstellt werden (Miyazaki & Fernandez, 2000).

Ungewollte Kontaktierung, Belästigung und Stalking: Die Vorgehensweise, Information über Konsumenten zu sammeln und mit diesem Wissen zu einem späteren Zeitpunkt unaufgefordert Kundenkontaktierungen vorzunehmen, ist seit Längerem Thema von Privacydiskussionen (Goodwin, 1991; Milne 1997; Miyazaki & Fernandez, 2000). Auch Privatpersonen können diese Informationen für Belästigungen oder sogar Stalking missbrauchen (Gross & Acquisti, 2005).

Herauslösung aus dem Kontext: Aus dem Kontext gelöste Textbausteine, Bilder oder Videosequenzen können eine völlig andere Bedeutung erhalten (Gasser et al., 2011). Ein berühmtes Beispiel hierfür ist ein im Internet veröffentlichtes Foto des US-Teenie-Stars Miley Cyrus im Jahre 2009 zusammen mit ihren Freunden, die ihre Augen mit den Fingern zu Schlitzaugen verengen. Schnell wurden rassistische Vorwürfe laut und das Bild wurde von der asiatisch-pazifischen Gemeinde als pure Provokation wahrgenommen und als Skandal durch alle Medien getragen. Miley Cyrus musste sich öffentlich für dieses Foto entschuldigen (Focus, 2009).

Internet Shaming: Internet-Shaming bezeichnet das öffentliche Anprangern von Personen oder Institutionen im Internet (Solove, 2007). Das wohl berühmteste Beispiel hierfür ist Star Wars Kid, der sich nach der millionenfachen Verlinkung seines Videos in psychiatrische Betreuung begab. Dies lässt eine Rückbesinnung auf die Tradition der Öffentlichmachung des 13. Jahrhunderts erkennen: "The shamer's explanation for attacking another person, somebody he probably didn't even know, stems from a belief that shame is necessary to ensure social order" (Solove, 2007, S. 102). Das öffentliche Anprangern hinterlässt Spuren, die den Betroffenen ein Leben lang begleiten können. Die Anonymität, aber auch die vielen Möglichkeiten und insbesondere die erhöhte Sichtbarkeit der Aktionen im Internet sind Gründe, dass An-

prangern zunimmt. Internet Shaming kann durch tausendfache Verlinkung von Texten, Videos oder Fotos geschehen und mit fiesen Kommentaren untermauert werden, welche einen nachhaltigen Reputationsschaden für die betreffende Person mit sich bringen kann (Gasser et al., 2011).

(3) Aggregation und Analyse

Erstellung von digitalen Dossiers: Kommerzielle Unternehmen, wie zum Beispiel RapLeaf, versuchen, digitale Dossiers von Personen zu erstellen. Dazu werden Daten über einen längeren Zeitraum aus verschiedenen Online-Geschäftsmodellen aggregiert, analysiert und geclustert – so kann ein persönliches Profil erstellt werden (Nissenbaum, 2009; Gross & Acquisti, 2005; Solove, 2004). Je umfassender die Datenaggregation, desto mehr muss auf potenzielle Risiken in Bezug auf Privacy geachtet werden. Solche digitalen Dossiers können missbraucht werden, um Individuen zu diskriminieren oder auszugrenzen. Sie bergen aber noch andere Risiken: unautorisierter Zugriff auf diese Dossiers können Stalking, Belästigungen oder Identitätsdiebstahl ermöglichen (Palfrey & Gasser, 2008; Marwick et al., 2010).

Identitätsdiebstahl: Beim Identitätsklau tritt eine Drittperson unter Namen und Adresse einer anderen Person auf – ohne deren Wissen oder Einverständnis (Gross & Acquisti, 2005). Durch Identitäts-Diebstähle können zum Beispiel Kreditkarten missbraucht, digitale Dossiers verschmutzt sowie Reputationsschäden angerichtet werden.

Studien zeigen, dass private Daten oftmals trotz Privacybedenken im Internet offengelegt werden (Youn, 2005; Norberg, Horne & Horne, 2007; Acquisti & Gross, 2007; Christofides et al., 2009; Belanger & Crossler, 2011). Dieses widersprüchliche Verhalten nennt Barnes (2006) das „Privacy-Paradox“. Barnes (2006) wie auch Norberg et al. (2007) argumentieren, dass dieses Paradox meistens bei Jugendlichen auftritt, welche die Dimensionen des Internets noch nicht abschätzen können. Acquisti und Gross (2007) erklären dieses Paradox damit, dass der Wunsch des Nutzers, seine Privacy zu schützen, nicht mit seinem tatsächlichen Verhalten übereinstimmt. Die Annahme, dass Nutzer sich keine oder weniger Gedanken über die Privacy ihrer Daten machen, weil sie so viele persönliche Daten online stellen, ist ein Trugschluss: Es besteht keine Korrelation zwischen der Bereitschaft, private Daten im Internet zu veröffentlichen, und der Bedenken bezüglich Privacy (Tufekci, 2008).

Welches Risiko Konsumenten einzugehen bereit sind, hängt davon ab, welche Vorteile sie durch die Bekanntgabe ihrer persönlichen Daten erhalten (Culnan, 2000). Chellappa und Sin (2005) argumentieren, dass Nutzer bereit sind, Informationen zur Verfügung zu stellen, wenn sie direkt von Vorteilen profitieren können. Der Austausch der Daten findet also nur statt, wenn der quantifizierte Wert der zur Verfügung gestellten Daten den durch die Personalisierung geschaffener Mehrwert nicht übersteigt. Es kann also sein, dass Kunden und Nutzer nicht an Online-Transaktionen teilnehmen, da ihnen der Verlust von Teilen ihrer Privacy zu riskant ist. Im Umkehrschluss werden Kunden ihre Daten dann zur Verfügung stellen, wenn das Bedürfnis nach Teilnahme grösser ist als das wahrgenommene Risiko eines Privacyverlustes.

Welche Faktoren die Privacybedenken der Nutzer beeinflussen und welche Strategien diesbezüglich auf Seiten der Nutzer und Unternehmen bestehen, wird im nächsten Kapitel behandelt.

2.2.3 Einflussfaktoren auf Privacybedenken und Strategien zum Schutz der Privacy

In den letzten Jahren ist eine erhöhte Sensibilität der Nutzer zu erkennen, wenn es um die Sammlung und Aggregation von persönlichen Daten geht. Medien und Verbraucherschutzorganisationen haben Privacy auf ihre Agenda gesetzt. Aber nicht nur die mediale Aufmerksamkeit, sondern auch die Politik, der Gesetzgeber und die Rechtsprechung, veränderte soziale Normen und Standards, der Bildungsstand einer Bevölkerung oder technologische Entwicklungen beeinflussen die Wahrnehmung von Privacy. Um die Herausforderungen von Privacy im digitalen Zeitalter zu analysieren, wird im folgenden Kapitel auf die beiden Hauptakteure, die Nutzer und die Anbieter von Online-Geschäftsmodellen, eingegangen.

2.2.3.1 Einflussfaktoren auf Privacybedenken

Um Privacybedenken zu beeinflussen und zu minimieren, ist es wichtig, deren Einflussfaktoren zu kennen. Die Wissenschaft hat fünf zentrale Einflussfaktoren auf Privacybedenken der Konsumenten identifiziert: (1) Bewusstsein, (2) Verwendung der Information, (3) die Informationssensibilität, (4) Vertrautheit mit dem Unternehmen und (5) Kompensation (Sheehan & Hoy, 2000; Phelps et al., 2000; Lanier & Saini, 2008), wie in Abbildung 15 dargestellt:

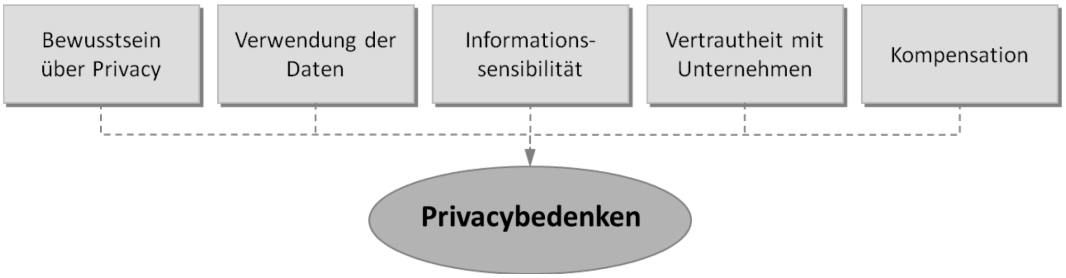


Abbildung 15: Einflussfaktoren auf Privacybedenken (Sheehan & Hoy, 2000; Phelps et al., 2000; Lanier & Saini, 2008)

Bewusstsein über Privacy: Wie ein Individuum Privacy im Internet wahrnimmt, ist sehr unterschiedlich und kommt auf persönliche Faktoren wie Alter, Geschlecht, Bildungsstand oder Internetkenntnisse an (Lewis, Kaufman & Christakis, 2008; Youn, 2005; Hargittai, 2002). Wissenschaftler gehen davon aus, dass das Bewusstsein für Datensicherheit bei den Konsumenten erst entsteht, wenn sie erfahren, dass ein Unternehmen Daten über sie sammelt, aggregiert und diese eventuell ohne ihre Einwilligung weiterverwendet (Sheehan & Hoy, 2000; Nowak & Phelps, 1995; Cespedes & Smith, 1993). Meistens merkt der Konsument dies erst, wenn unerwünschte Werbung oder Spam bei ihm eintreffen. Unternehmen bieten meistens Wahlmöglichkeiten in Form von Opt-in- oder Opt-out-Optionen[19] an, bei denen der Kunde entscheiden kann, ob seine persönlichen Daten gespeichert werden dürfen oder nicht, und informieren gleichzeitig über die Verwendung der Daten (Milne & Rohm, 2000). Diese Wahlmöglichkeit ist wichtig, denn der Kunde ist weniger über Datensicherheit besorgt, wenn Unternehmen um Erlaubnis fragen (Nowak & Phelps, 1995).

[19] Opt-in- oder Opt-out-Option bedeutet, dass der Nutzer die Wahl hat, ob er vom Unternehmen kontaktiert werden will oder nicht. Opt-in bedeutet, dass er explizit danach befragt wird (per Telefon oder durch einen Button bei der Anmeldung). Opt-out bedeutet automatische Aufnahme in die Verteilliste, der Nutzer muss explizit den Wunsch anbringen, von der Verteilerliste gelöscht zu werden.

Verwendung der Daten: Ein Hauptanliegen der Kunden ist, dass sie wissen wollen, wozu ihre Daten verwendet werden und dass ihre Daten nicht zweckentfremdet oder an Dritte weitergegeben werden (Nowak & Phelps, 1995). Konsumenten werden verunsichert, wenn sie keine Kontrolle über ihre Daten haben und nicht wissen, ob ihre Daten weiterverwendet werden oder nicht (Sheehan & Hoy, 2000; Belanger & Hiller, 2006; Sheehan & Hoy, 2000). Die Zweitverwendung von privaten Daten wird oft als Eingriff in die Privacy wahrgenommen, besonders wenn Konsumenten nicht darauf aufmerksam gemacht werden (Cespedes & Smith, 1993; Phelps et al., 2000; Wang & Petrison, 1993).

Informationssensibilität: Nicht alle Daten sind gleich delikat, der Nutzer macht Unterschiede, welche Daten er als privat und somit als sensibel erachtet und welche er öffentlich preisgeben will (Milne, 1997; Livingstone, 2008; Chellappa & Sin, 2005). Die Sensibilität der Daten, definiert als die wahrgenommene Intimität der Daten, hat einen grossen Einfluss auf die Bereitschaft, diese zur Verfügung zu stellen (Premazzi et al., 2010; Westin, 2003; Andrade et al., 2002). Sensibilität ist kontextabhängig; je nach Person und Situation können Daten als mehr oder weniger sensibel wahrgenommen werden (Cranor, Reagle & Ackermann, 2000; Nowak & Phelps, 1992; Milne, 1997). Es kommt auf die Form und den Inhalt der Daten an, aber ebenso darauf, wie die jeweilige Person die Daten einschätzt (Gandy, 1993; Jones, 1991; Wang & Petrison, 1993). Je stärker eine Person ihre Daten als sensibel einstuft, desto mehr Privacybedenken hat sie (Gandy, 1993; Sheehan & Hoy, 2000; Phelps et al., 2000). Gandy (1993) zeigt in seiner Studie, dass Menschen Informationen dann als sensibel einstufen, wenn sie denken, die Veröffentlichung der jeweiligen Informationen könnte ihnen Schaden zufügen.

Die Privacy-Literatur unterscheidet zwischen Marktdatensätzen (Market-Level Information oder auch Modeled Data) und individual spezifischen Daten (Individual Specific Information). Marktdatensätze sind Konsumentendaten, welche die Charakteristik einer spezifischen Kundengruppe, eines Marktsegmentes, einer bestimmten Zielgruppe eines Mediums oder einer geografischen Region beschreiben. Laut Nowak und Phelps (1992, 1995) sind aber nicht Marktdatensätze sondern persönliche, individual-spezifische Informationen die primäre Quelle für Privacybedenken (Culnan, 2000; Phelps et al., 2000; Nowak & Phelps, 1992, 1995, 1997; Vidmar & Flaherty, 1985). Die Daten von identifizierbaren Individuen können in fünf Hauptkategorien eingeteilt werden. (1) Demografische Merkmale (Alter, Zivilstand, Geschlecht, Beruf, Bildung), (2) Lifestyle-Merkmale (Medienverhalten, Freizeitverhalten), (3) Einkaufs-

präferenzen (Kaufhistorie, Markenpräferenzen, Kauffrequenzen, Haushaltseinkommen, Einkaufssummen), (4) finanzielle Daten (Kreditkarten- und Bankinformationen, Kreditwürdigkeit) und (5) persönliche Identifikatoren (Name, Adresse, Sozialversicherungsnummer) (Jackson & Wang, 1994; Nash, 1993).

Eine Studie mit über 9'000 Teilnehmern, durchgeführt von Nokia Siemens Networks, konnte bestätigen, dass grosse Unterschiede in der Wahrnehmung der Sensibilität von Daten bestehen (Abbildung 16). Als höchst sensibel zum Beispiel gelten Kreditkartennummer, Sozialversicherungsnummer, Passwörter von Online-Communitys und die Kreditwürdigkeit. Als immer noch sensibel werden persönliche Kontaktlisten, Einkommensdaten, Adresse, Fotos oder Krankheitsakten eingestuft. Beruf, Hobbys, Zivilstand oder Altersklasse hingegen werden als völlig unsensible Daten eingestuft. Je präziser die abgefragten Daten, desto besorgter waren die Befragten. Man ist also bereit, die Altersklasse und den Beruf anzugeben, nicht aber die Kreditkarten- oder Sozialversicherungsnummer (Nokia Siemens Networks, 2009).

Abbildung 16: Sensibilität von persönlichen Daten (eigene Darstellung in Anlehnung an Nokia Siemens Networks, 2009)

Chellappa und Sin (2005) konnten in ihrer Forschung aufzeigen, dass nicht nur Daten, die Rückschlüsse auf die Identität der Nutzer erlauben, als heikel empfunden werden, sondern dass auch anonyme und nicht persönliche Informationen Bedenken auslösen können. Dies mag daran liegen, dass Kunden- und Nutzerprofile durch die Aggregation unterschiedlichster Daten generiert werden und dass die Möglichkeit besteht, anonyme Daten trotzdem mit dem Profil in Verbindung zu bringen. Anbieter von Online-Geschäftsmodellen sollten sich bewusst sein, dass Nutzer und Kunden auf persönliche wie auch auf anonyme Daten, die vom Anbieter gespeichert und weiterverwendet werden, sensibel reagieren können (Chellappa & Sin, 2005).

Vertrautheit mit dem Unternehmen: Je vertrauter eine Person mit dem Unternehmen ist und je langfristiger die Beziehung ist, desto kleiner sind die Bedenken bezüglich der Sicherheit ihrer persönlichen Daten (Phelps et al., 2001; Sheehan & Hoy, 2000). Sheehan und Hoy (2000) fanden heraus, dass die Art der Beziehung (langfristig vs. kurzfristig) einen direkten Einfluss darauf hat, welche Arten von Informationen ein Kunde zur Verfügung stellt. Ein zentraler Aspekt von Vertrautheit ist das Vertrauen selbst (Vidmar & Flaherty, 1985). Wie Vertrauen entsteht und wie es gefördert werden kann, wird im Kapitel 2.3 vertieft behandelt.

Kompensation: Im Mittelpunkt der meisten Bedenken steht das Austauschverhältnis zwischen dem Nutzen der Bekanntgabe der persönlichen Daten und den Kosten, die man dafür in Kauf nehmen muss (Hoffman et al., 1999b; Ashworth & Free, 2006; Westin, 1967; Laufer & Wolfe, 1977). Die Privacy-Calculus-Theorie geht ebenfalls von diesem Austauschverhältnis aus: Der Nutzen muss höher sein als das Risiko, welches man durch die Preisgabe der Daten eingeht (Krasnova et al., 2010). Konsumenten ordnen jeder Information einen gewissen Wert zu und geben diese Information nur preis, wenn der Nutzen dafür höher ist als die Kosten (Ashworth & Free 2006; Dunfee, Smith & Ross, 1999; Chellappa & Sin, 2005). Der Nutzen kann einen finanziellen Wert haben (in Form einer monetären Vergütung oder von Produkten oder Dienstleistungen) oder informationsbasiert sein (Zugang zu Information) (Sheehan & Hoy, 2000). Verschiedene Autoren weisen darauf hin, dass eine Entschädigung für den Austausch der persönlichen Daten einen direkten Einfluss auf Datenschutzbedenken haben kann (Chellappa & Sin, 2005; Vidmar & Flaherty, 1985; Goodwin, 1991; Milne & Gordon, 1993; Sheehan & Hoy, 2000). Solove schreibt hierzu: "People are quick to say in the abstract that they want privacy, but when offered money or discounts in return for their personal information, they readily relinquish it" (2004, S. 80 f.). Besonders der wahrgenommene Nutzen der Pflege von sozialen Beziehungen im Netz wird gemäss Christofides et al. (2009) höher eingeschätzt als das durch die bereitgestellten Daten eingegangene Risiko. Im Kapitel 2.1 wurde darauf verwiesen, dass persönliche Daten die neue Währung des Internets sind. Entsprechend können Unternehmen durch angemessene Kompensation erreichen, dass Kunden die gewünschte Information zur Verfügung stellen (Milne & Gordon, 1993). Der persönlich wahrgenommene Nutzen oder Gewinn muss also grösser sein als der mögliche Verlust der Privacy, wenn die zur Verfügung gestellten Daten veröffentlicht würden (Culnan & Bies, 2003).

Weitere Einflussfaktoren: In ihrer Studie konnten Sheehan und Hoy (2000) nachweisen, dass die oben vorgestellten fünf Einflussfaktoren die grössten Bedenken der Konsumenten abdecken. Zusätzlich beeinflussen Faktoren wie Geschlecht, Alter (Taraszow et al., 2010; Nosko et al., 2010) oder Einkommen, die soziokulturelle Zugehörigkeit der Internetnutzer, die eLiteracy (Bawden & Robinson, 2008; Bawden, 2001; Hargittai, 2002), aber auch die Beziehung zwischen dem Unternehmen und dem Nutzer sowie der Austausch von Information zwischen den beiden Parteien die Privacybedenken (Culnan, 1995; Culnan & Armstrong, 1999; Sheehan, 1999; Sheehan & Hoy, 2000).

In diesem Kapitel wurde aufgezeigt, welche Faktoren Einfluss auf die Privacybedenken der Nutzer haben. Im folgenden Kapitel wird darauf eingegangen, welche Strategien zum Schutz der Privacy bestehen, einerseits aus der Nutzerperspektive, aber ebenso von Seiten der Unternehmen.

2.2.3.2 Nutzerstrategien zum Schutz der Privacy

Die Nutzer wollen Kontrolle über die Sammlung, Verbreitung und den Gebrauch ihrer persönlichen Daten (Goodwin, 1991; Milne & Boza, 1999; Phelps et al., 2000; Lanier & Saini, 2008). Besonders im Internet sind Nutzer auf sich alleine gestellt, wenn es darum geht, ihre persönlichen Daten zu managen und zu schützen. Wie kann man als Nutzer seine Daten schützen und was kann man gegen ungewollten Zugriff auf seine persönlichen Daten tun?

Die Studie von Raman und Pashupati (2005) unterscheidet zwei Strategien zum Schutz der Privacy: die „Avoidance Strategy“ sowie der „Confrontive Approach“. Personen, welche die Vermeidungsstrategie verfolgen, verhalten sich defensiv, das heisst, sie meiden ganz einfach bestimmte Webseiten, um möglichst wenig Information über sich selbst zur Verfügung zu stellen. Der konfrontative Ansatz konzentriert sich auf Problemlösungsansätze. Verhaltensweisen zum Schutz der Privacy sind (1) Informationssuche, (2) Verschleierungspraktiken, (3) Privacy-Einstellungen anpassen oder (4) seine Rechte auszuüben (Youn, 2009; Milne & Rohm, 2000; Milne & Culnan, 2004; Marvick, Diaz & Palfrey, 2010), wie in Abbildung 17 dargestellt:

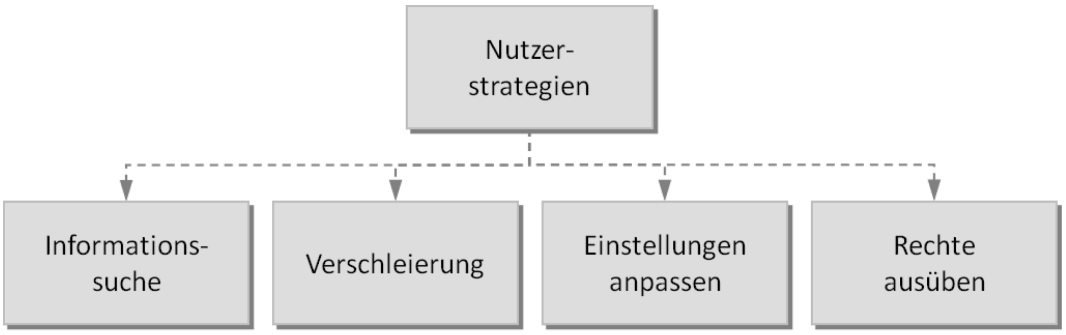


Abbildung 17: Konfrontative Nutzerstrategien zum Schutz der Privacy (eigene Darstellung)

Informationssuche: Die Nutzer wollen wissen, wer welche Daten zu welchem Zweck sammelt (Lanier & Saini, 2008; Dommeyer & Gross, 2003; Milne & Culnan, 2004; Nowak & Phelps 1995). Internetnutzer informieren sich bei besser informierten Freunden und suchen in Communitys und Foren nach Lösungen (Buchmann, Böhm & Raabe, 2008). Das Lesen der Datenschutzrichtlinien ist ein Weg, sich Wissen und somit Verständnis über Datenschutz und Privacy anzueignen (Milne & Rohm, 2000). Dies kann dazu führen, dass der Nutzer das Gefühl hat, mehr Kontrolle über seine eigenen Daten zu besitzen, denn nach dem Lesen der Datenschutzrichtlinien kann er entscheiden, ob er seine Daten zur Verfügung stellen will oder nicht (Wang et al., 2004; Milne & Culnan, 2004). Trotzdem achtet der Grossteil der Internetnutzer, besonders Digital Natives, nicht auf Datenschutzrichtlinien und liest diese auch nicht (Taraszow et al., 2010; Milne, Rohm & Bahl, 2004; Marvick, Diaz & Palfrey, 2010). Youn (2005) konnte in ihrer Studie feststellen, dass sich Nutzer mit mehr Erfahrung in den Sozialen Medien eher Gedanken zu der Privacy ihrer Daten machen und demnach auch eher bereit sind, die Datenschutzrichtlinien zu lesen. Steeves und Webster (2008, S. 8) resümieren, dass 49 % der in der Studie befragten Probanden noch nie eine Datenschutzerklärung im Internet gelesen haben und 50 % trotz Kenntnis der Richtlinien ihr Verhalten nicht geändert oder angepasst haben.

Verschleierung: Konsumenten können wählen, ob sie gegenüber Unternehmen ihre wahre Identität oder nur Teile davon preisgeben oder ob sie vollkommen anonym bleiben möchten (Zwick & Dholakia, 2004; Chen & Rea, 2004): „Die Datensammlungen der Firmen quellen über vor Donald Ducks, die in Bahnhofsstrassen und Parkalleen wohnen und fantasievolle E-Mail-Adressen und Telefonnummern besitzen. Die Firmen haben viel zu viele nutzlose Daten“ (Bäumler, 2000, S. 133). Das Angeben von falschen oder unvollständigen Informationen, das Führen mehrerer Profile oder die Verweigerung der Preisgabe gewisser Daten werden als Strategie angesehen, um nicht allzu sehr von Marketingfirmen und Werbeagenturen belästigt

zu werden (Grant, 2006). Sheehan und Hoy (1999) haben festgestellt, dass zwischen Datensicherheitsbedenken und Online-Datenschutzverhalten eine starke positive Beziehung besteht. Je mehr Datensicherheitsbedenken, desto mehr versuchen Nutzer, ihre persönlichen Daten im Netz zu schützen, indem sie falsche und unvollständige Angaben zur Verfügung stellten (Moscardelli & Divine, 2007). Youn (2005) fand in ihrer Studie heraus, dass 53 % der Befragten bei kommerziellen Webseiten unvollständige Informationen hinterliessen, während 44 % falsche Informationen angaben und 43 % der Probanden die Seite verliessen, ohne persönliche Angaben von sich zur Verfügung zu stellen. Insgesamt 43 % gaben an, auf andere Seiten auszuweichen, falls zu viele Informationen abgefragt wurden. Steeves und Webster (2008) stellten in ihrer Untersuchung fest, dass 59 % der 3'000 Befragten schon mindestens einmal ein falsches Alter angegeben haben, während 26 % bereits eine andere Identität angenommen haben und 23 % ihr äusseres Erscheinungsbild angepasst haben. Dies geschah aber nicht nur aus Gründen der Datensicherheit, sondern auch aus Neugierde, um zu sehen, wie es ist, älter oder jünger zu sein, um zu flirten oder um Neigungen auszuleben (Steeves & Wing, 2005).

Privacyeinstellungen anpassen und verändern: Um die eigene Privacy zu schützen, müssen gewisse Kenntnisse über Privacy und Internetfähigkeiten vorhanden sein, ansonsten können Nutzer ihre Privacyeinstellungen nur schwer personalisieren und verändern. Lenhart, Madden, Macgill und Smith (2007) konnten aufzeigen, dass Digital Natives restriktiver mit ihren persönlichen Daten umgehen als Digital Immigrants. 39 % der jüngeren Nutzer gaben an, dass wenn sie Fotos ins Internet hochladen, sie die Zugriffsmöglichkeiten von Drittpersonen grösstenteils limitierten, 38 % den Zugriff manchmal und 21 % gar nie limitierten. Nur 34 % der Erwachsenen schränkten den Zugriff auf ihre Fotos meistens ein, 24 % manchmal und 39 % gaben an, dass sie ihre Daten gar nicht schützten.

Rechte ausüben und auf die Löschung von Informationen bestehen: Internetnutzer können sich zwar auf bestehende Datenschutzgesetze und Richtlinien verlassen (Youn, 2005), sie müssen sich aber aktiv um die Löschung von Informationen wie Namen oder E-Mails kümmern und Opt-out-Funktionen aktivieren. Eine Umfrage zur Kenntnis des Vorgehens bei der Löschung von Kundendaten hat ergeben, dass 52 % der Befragten keine Kenntnisse über den Ablauf des Prozesses besitzen (Culnan, 1995).

Es bestehen unzählige **weitere Strategien** zum Schutz der Privacy, wie zum Beispiel das Nutzen von verschlüsselten Seiten, das Führen mehrerer Mailadressen, das

Chiffrieren von E-Mails oder die Überwachung der Bankkonten. Die in diesem Kapitel behandelte Aufzählung von Strategien ist nicht als abschliessend zu betrachten.

Trotz Vorsichtsmassnahmen und Strategien zum Schutz der Privacy kann der Nutzer wenig unternehmen, um seine persönlichen Informationen zu schützen, wenn seine privaten Daten erst einmal gesammelt, aggregiert und verbreitet sind (Lanier & Saini, 2008). Deshalb ist es für Unternehmen umso wichtiger und zunehmend ein Abgrenzungsmerkmal, sich im Bereich der Datensicherheit und Privacy ihrer Kunden zu profilieren. Im nächsten Kapitel wird deshalb vertieft darauf eingegangen, wie Unternehmen den Schutz der Privacy ihrer Kunden gewährleisten können.

2.2.3.3 Firmeninitiativen zur Reduktion von Privacybedenken

Nutzer von Online-Geschäftsmodellen stellen in den letzten Jahren in Bezug auf die Verwendung und den Umgang mit persönlichen Daten klare Forderungen an die Unternehmen. Ein fairer und transparenter Umgang mit Kundendaten gilt heute als zentrales Profilierungsmerkmal von Anbietern von Online-Geschäftsmodellen (Ashworth & Free, 2006). Deshalb wird im Folgenden die Privacy aus der Unternehmensperspektive beleuchtet und insbesondere darauf eingegangen, wie Unternehmen die Bedenken der Nutzer reduzieren können.

Geschäftsbeziehungen basieren auf einem Austauschverhältnis: Personalisierte Kommunikation, massgeschneiderte Angebote sowie besserer Kundenservice sind nur möglich, wenn Kunden bereit sind, dem Unternehmen persönliche Daten zur Verfügung zu stellen (Rust et al., 2002). Marktorientierte Unternehmen stehen somit in einem Interessenskonflikt: Auf der einen Seite streben sie erhöhten Kundenservice durch die Sammlung und Aggregation persönlicher Informationen an, während sie auf der anderen Seite rechtliche und persönliche Datensicherheitsbedenken adressieren und reduzieren möchten (Novak & Phelps, 1997). Wichtig ist, dass Unternehmen beim Management der Privacy ihrer Kunden nicht nur versuchen, deren Bedenken zu minimieren, sondern, dass durch einen professionellen Umgang mit Kundendaten die Rahmenbedingungen für nachhaltigen Erfolg des Unternehmens geschaffen werden (Sarathy & Robertson, 2003; Lanier & Saini, 2008). Die Frage ist, wie eine Volkswirtschaft die Privacy der Konsumenten effizient, umfassend und gerecht organisieren kann. Ziel ist es, einen optimalen Schutz zu ermöglichen, ohne übermässig in die bestehenden Geschäftspraktiken der Unternehmen eingreifen zu müssen (Bo-

wie & Jamal, 2006). Die Herausforderung für Unternehmen besteht nun darin, die Handhabung der Privacy mit den eigenen Bedürfnissen, mit den Bedürfnissen der Kunden sowie den juristischen Anforderungen in Einklang zu bringen (Lanier & Saini, 2008). Unternehmen können dieser Herausforderung von zwei Seiten her begegnen: Sie können einerseits die Privacybedenken ihrer Kunden aktiv adressieren und versuchen, diese abzubauen, oder sie können andererseits versuchen, Vertrauen aufzubauen (Milne & Boza, 1999; Culnan & Armstrong, 1999; Chellappa & Sin, 2005; Schoenbachler & Gordon, 2002; Wang & Petrison, 1993), wie in Abbildung 18 grafisch dargestellt.

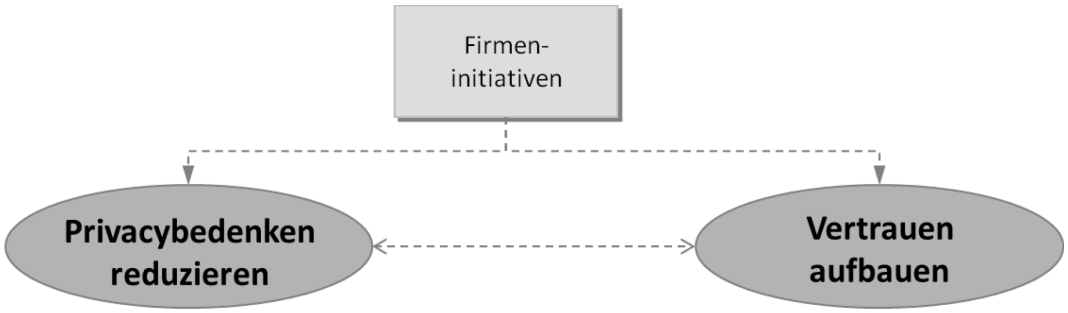


Abbildung 18: Unternehmen können Privacybedenken reduzieren oder Vertrauen aufbauen (eigene Darstellung)

Je mehr ein Nutzer dem Unternehmen vertraut, desto kleiner sind dessen Bedenken und desto grösser die Bereitschaft, persönliche Daten zur Verfügung zu stellen (Schoenbachler & Gordon, 2002; Milne & Boza, 1999; Culnan & Armstrong, 1999; Olivero & Lunt, 2004; Chellappa & Sin, 2005). Im Folgenden wird auf die Reduktion der Privacybedenken eingegangen, Vertrauen wird im Kapitel 2.3 im Detail behandelt.

Im Jahre 1998 nahm die Federal Trade Commission (FTC) Untersuchungen zur Selbstregulierung von Privacy im Internet (FTC, 1998) vor (Culnan, 2000) und stellte diesen Report dem US-Kongress zur Verfügung. Der Bericht argumentiert, dass die Privacy der Nutzer garantiert sein muss, um das Potenzial von Online-Geschäftsmodellen ausnutzen zu können. Die Untersuchungen der FTC ergaben, dass mehr als 85 % aller kommerziellen Websites persönliche Kundeninformationen sammeln, aber nur 14 % der Unternehmen die Kunden über diese Datensammlung informierten. Nur gerade 2 % der untersuchten Unternehmen informierte ihre Kunden durch umfassende Datenschutzrichtlinien. Aufgrund dieser alarmierenden Zahlen stellte die FTC die Fair Information Practices (FIP) zusammen. Die FIP sind Grundsatzerklärungen zur Sammlung und Nutzung von persönlichen Informationen

und werden als Grundlage vieler internationaler Datenschutzgesetze verwendet (Culnan, 2000; Lanier & Saini, 2008; Culnan & Armstrong, 1999). Die FIP beinhalten die folgenden vier Grundsätze: (1) den Kunden informieren, (2) die Einwilligung des Kunden einholen, (3) dem Kunden Einsicht über die Daten gewähren und (4) Sicherheit gewährleisten (FTC, 2000). Diese vier Firmeninitiativen zur Reduktion von Privacybedenken sind in Abbildung 19 zusammengefasst:

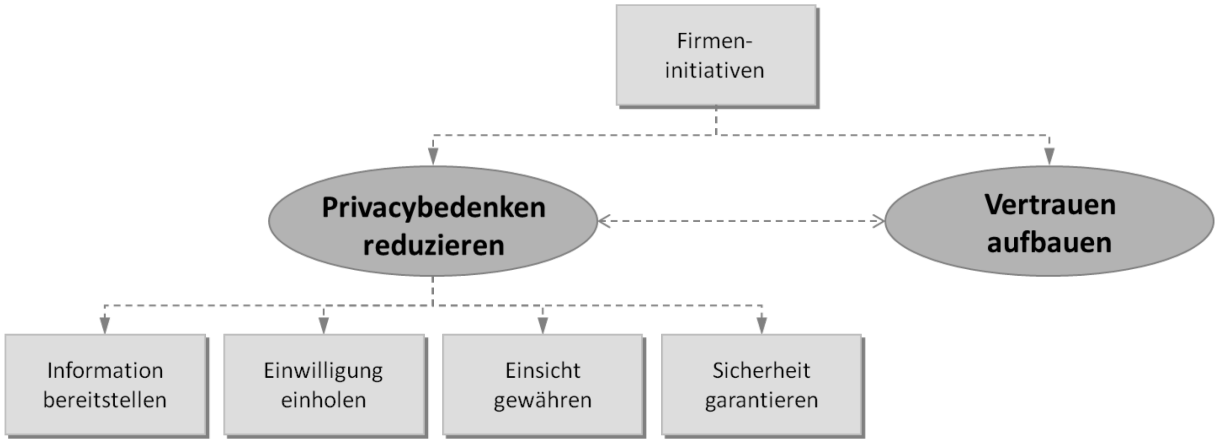


Abbildung 19: Firmeninitiativen zur Reduktion von Privacybedenken der Nutzer (FTC, 2000; Milne & Boza, 1999; Culnan & Armstrong, 1999)

Nutzer informieren: Nutzer haben das Recht zu wissen, dass ihre Daten gesammelt und wie diese verwendet werden. Unternehmen müssen ihre Informationspraktiken transparent kommunizieren und glaubwürdig aufzeigen, wie diese gesammelten Daten vor dem Zugriff Dritter geschützt werden (FTC, 2000; Culnan & Armstrong, 1999; Hoy & Phelps, 2003). Ziel ist es nicht, den Nutzer mit Informationen zu überschwemmen, sondern diesen in verständlichen und einfachen Sätzen über die Sachlage zu informieren.

Einwilligung des Nutzers einholen: Die Nutzer sind sich zum grossen Teil bewusst, dass Daten über sie gesammelt werden. Bedenken diesbezüglich können gemindert werden, indem um Erlaubnis gefragt wird, ob die Information für das Unternehmen genutzt oder an Dritte weitergegeben werden darf (FTC, 2000). Dies kann entweder explizit oder per Default geschehen (Ashworth & Free, 2006; Nowak & Phelps, 1995; Sheehan & Hoy, 2000). Durch das Einholen einer Einwilligung zur Verwendung der Daten wird der Nutzer einerseits über die vorhandenen Daten informiert und ihm wird die Verfügungsgewalt und Kontrolle über seine persönlichen Daten zugestanden (Phelps et al., 2000).

Einsicht in die Daten gewähren: Konsumenten haben das Gefühl, immer mehr die Kontrolle über ihre Daten und deren Verwendung zu verlieren. Sie finden es unakzeptabel, dass Marketer diese Informationen ohne ihr Wissen an Dritte weitergeben (Nowak & Phelps, 1992; Sheehan & Hoy, 2000). Deshalb sollten Unternehmen ihren Kunden jederzeit Einsicht über die gesammelten Daten gewähren und den Nutzern die Möglichkeit geben, eine Datenlöschung zu beantragen (FTC, 2000; Culnan & Armstrong, 1999). Culnan (1995) konnte aufzeigen, dass Nutzer, welche wissen, wie sie eine Datenlöschung beantragen können, weniger Privacybedenken haben. Bereits vor 100 Jahren kommentierte der Richter Louis Brandeis die Wichtigkeit der Offenlegung und Transparenz mit den Worten: "Sunlight is said to be the best of all disinfectants." (Brandeis, 1914, S. 92).

Sicherheit: Nutzer wollen eine Garantie der jeweiligen Firmen dafür, dass ihre Daten sicher verwahrt und vor dem Zugriff unbefugter Dritter geschützt sind (Lanier & Saini, 2008; Hoy & Phelps, 2003; Jones, 1991; Miyazaki & Fernandez, 2000). Die Sicherheit der Nutzer wird vor allem durch Fehler oder Manipulationen der IT-Systeme eines Transaktionspartners gefährdet (Friedman, Kahn & Howe, 2000; Urban et al., 2009). Die Pflege einer angemessenen Infrastruktur und effektive Managementprozesse können die Sicherheit der Beteiligten schützen und erhöhen (Belanger et al., 2002). Unternehmen sollten in ihrer „Privacy Policy" den Schutz der Privacy ihrer Kunden garantieren. Darin sollten Angaben über den Gebrauch und die Verbreitung aller angegebenen persönlichen Daten enthalten sein (Egger, 2001) und aufgezeigt werden, welche Regressmöglichkeiten bestehen, falls die Daten nicht wie vereinbart gehandhabt werden (FTC, 2000). Die Literaturrecherche ergab, dass Anbieter von Online-Geschäftsmodellen noch immer keinen genügenden Schutz der Privacy ihrer Nutzer bieten: Viele Unternehmen haben keine oder ungenügende Privacy Policies (Peslak, 2005; Sheehan 2005; Belanger & Crossler, 2011).

In diesem Kapitel wurde aufgezeigt, dass unterschiedliche rechtliche, betriebswirtschaftliche und technologische Lösungen entwickelt wurden, um die Privacy zu schützen und Bedenken zu verringern; trotzdem bleibt eine gewisse Unsicherheit bestehen (Foxman & Kilcoyne, 1993; Goodwin, 1991; Phelps et al., 2000). Unternehmen müssen einen optimalen Schutz der Privacy garantieren können, um die Angst der Nutzer zu mildern und gleichzeitig Vertrauen aufbauen. Milne und Boza (1999) sowie Culnan und Armstrong (1999) konnten nachweisen, dass bei der Verwaltung von Kundeninformationen der Aufbau von Vertrauen effektiver ist, als auf die einzelnen Privacybedenken der Kunden einzugehen. Denn die Überzeugung, dass die

Sicherheitsmassnahmen und Richtlinien auch eingehalten werden, basiert immer auf Vertrauen. Deshalb bezeichnen viele Autoren mangelndes Vertrauen auch als das Hindernis beim Wachstum von Online-Geschäftsmodellen (Hoffman et al., 1999a; McKnight et al., 2002a; Urban et al., 2009).

Infolgedessen befasst sich das nächste Kapitel umfassend mit dem Management von Vertrauen und dem Einfluss von Vertrauen im Umfeld von Online-Geschäftsmodellen.

2.2.4 Zusammenfassung

Auch mehr als hundert Jahre nach der Definition von Warren und Brandeis (1890) gibt es keine allgemein akzeptierte Definition von Privacy. Zusammenfassend kann gesagt werden, dass das Konzept und somit die Definition von Privacy ein umfassendes Konstrukt ist. Es zeigt sich, dass Privacy noch immer ein umstrittenes Thema ist, welches gleichermassen von Behörden, Politik, Entscheidungsträgern, privaten Organisationen, Wirtschaft sowie von Bürgerinnen und Bürgern diskutiert wird (Lanier & Saini, 2008). Das Thema Privacy hat nichts an Relevanz verloren; ganz im Gegenteil, Privacy wird durch die sich verändernden Medien neu definiert und gewinnt durch die Verfügbarkeit von Nutzerinformationen im Internet weiter an Bedeutung. Die Teilnahme an Online-Transaktionen setzt stets ein Eingeständnis der Privacy voraus – jedoch in sehr unterschiedlichen Ausmassen (Rust et al., 2002). Es muss eine Balance gefunden werden zwischen der Sicherung von Privacy und der Wahl, seine persönlichen Daten freizugeben und zu verwalten.

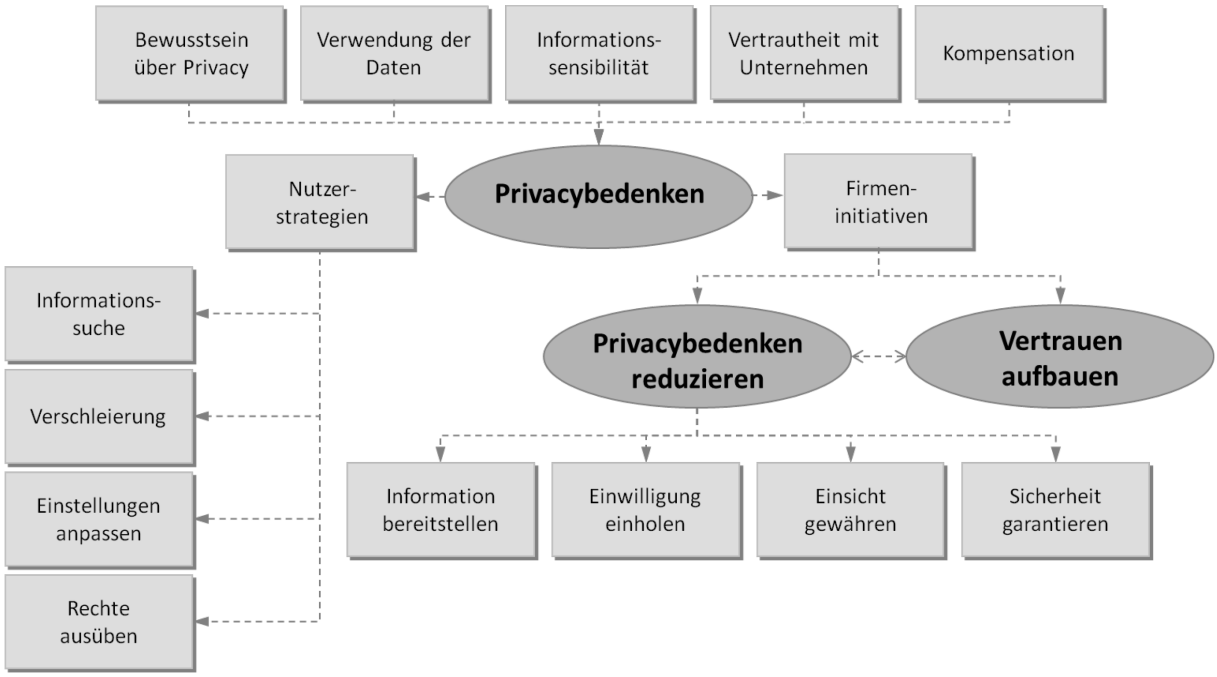


Abbildung 20: Zusammenhang von Privacybedenken, Nutzerstrategien und Firmeninitiativen (eigene Darstellung)

Der Zusammenhang zwischen dem Aufkommen von Informationstechnologien, welche die Digitalisierung und Verbreitung von jeder Form von Information möglich gemacht hat, und der Zunahme an Bedenken bezüglich der Privacy von Privatpersonen, Organisationen sowie dem Staat ist gut erforscht und dokumentiert (Lanier & Saini, 2008; Ashworth & Free, 2006; Milne, 2000; Peslak, 2005). Die Literatur identifiziert fünf Einflussfaktoren auf Privacybedenken: (1) Bewusstsein, (2) Verwendung der Information, (3) die Informationssensibilität, (4) Vertrautheit mit dem Unternehmen und (5) Kompensation (Sheehan & Hoy, 2000; Phelps et al., 2000; Lanier & Saini, 2008). Internetnutzer und Anbieter von Online-Geschäftsmodellen begegnen diesen Bedenken unterschiedlich. Nutzer versuchen, die Kontrolle über ihre Daten zu behalten, indem sie vier Verhaltensweisen befolgen: (1) Informationssuche, (2) Verschleierungspraktiken, (3) Privacy Einstellungen anpassen oder (4) ihre Rechte ausüben (Youn, 2009; Milne & Rohm, 2000; Milne & Culnan, 2004; Marvick, Diaz & Palfrey, 2010). Anbieter haben ebenfalls vier Möglichkeiten zur Reduktion von Privacybedenken zur Verfügung: (1) den Kunden informieren, (2) die Einwilligung des Kunden einholen, (3) dem Kunden Einsicht über die Daten gewähren und (4) Sicherheit gewährleisten (FTC, 2000). Effektiver als Bedenken abzubauen ist es jedoch, Vertrauen aufzubauen (Milne & Boza, 1999; Culnan & Armstrong, 1999). Der Gesamtzusammenhang zwischen Privacybedenken, Nutzerstrategien und Firmeninitiativen ist in Abbildung 20 dargestellt.

2.3 Die Lösung: Vertrauen aufbauen

Das Vertrauen in wirtschaftliche, politische und rechtliche Institutionen hat es möglich gemacht, dass arbeitsteilige Gesellschaften entstanden sind. Ein massiver Vertrauensverlust in diese komplexen Systeme würde zu einem zivilisatorisch-ökonomischen Rückschritt führen (Enzweiler, 2008). Der US-Ölmagnat Getty beschrieb es folgendermassen: „Wenn man einem Menschen trauen kann, erübrigt sich ein Vertrag. Wenn man ihm nicht trauen kann, ist ein Vertrag nutzlos." (ohne Datum). Vertrauen kreiert das soziale Umfeld, innerhalb dessen der Austausch funktionieren kann (Fukuyama, 1995; Luhmann, 1979). Das System der Marktwirtschaft ist ohne Vertrauen kaum denkbar, denn wenn der Einzelne nicht erkennen kann, woher ein Produkt stammt oder wie es sich zusammensetzt, dann muss er sich auf das Fachwissen und die Ehrlichkeit der Experten verlassen (Enzweiler, 2008). Vertrauen kann demnach als „Schmiermittel" der Gesellschaft bezeichnet werden (Hank, 2008). Vertrauensforscher haben einen langen Weg hinter sich und es existiert eine Vielzahl von vertrauensbildenden Modellen und Konzepten. Die Forscher sind sich darin einig, dass Vertrauen eine substanzielle Auswirkung auf jede Art von Transaktion hat (Fukuyama, 1995; Moorman et al., 1993; Morgan & Hunt, 1994). Insbesondere im Online-Bereich kommt Vertrauen eine gesteigerte Bedeutung zu (McKnight et al., 2002a). Ohne die freiwillige Beteiligung der Nutzer kann das Internet nicht sein volles Wertschöpfungspotenzial für Wirtschaft, Kultur und Gesellschaft entfalten. Insbesondere Online-Unternehmen sehen sich mit der Herausforderung konfrontiert, das Vertrauen ihrer Nutzer zu gewinnen und zu pflegen. Doch was genau ist Vertrauen in einer virtuellen Welt? Wie kann Vertrauen aufgebaut werden und welches sind die Faktoren, die das Nutzervertrauen im Netz beeinflussen? Wenn Nutzer dem Anbieter vertrauen, sind positive Transaktionsabsichten dann wahrscheinlicher?

Diesen Fragen geht das aktuelle Kapitel nach, ausserdem werden die wichtigsten Erkenntnisse der Vertrauensforschung aufgezeigt. Im ersten Kapitel 2.3.1 wird in das Thema Vertrauen eingeleitet und die zentralen Begriffe werden definitorisch abgegrenzt. Das zweite Kapitel 2.3.2 widmet sich der Entstehung von Vertrauen und diskutiert die Einflussfaktoren auf Vertrauen. Das dritte Kapitel 2.3.3 widmet sich der zukünftigen Absicht zu vertrauen und das letzte Kapitel 2.3.4 fasst die Erkenntnisse zusammen.

2.3.1 Einführung in das Thema Vertrauen und definitorische Abgrenzung

In diesem Kapitel soll als Erstes beantwortet werden, was Vertrauen genau ist und wie Vertrauen definiert wird (Kapitel 2.3.1.1). Das zweite Kapitel 2.3.1.2 widmet sich der Vertrauensforschung im Internet und das dritte Kapitel 2.3.1.3 geht auf die Bedeutung von Vertrauen für Anbieter von Online-Geschäftsmodellen ein.

2.3.1.1 Definition Vertrauen

Bis heute besteht keine allgemein akzeptierte Definition von Vertrauen (Urban et al., 2009). Über verschiedene Disziplinen hinweg sind sich Forscher jedoch einig, dass Vertrauen als eine Erwartungshaltung, eine Überzeugung oder ein Gefühl der Betroffenen verstanden wird (Belanger et al., 2002; Lee & Turban, 2001; McKnight et al., 2002a) und sich aus den Komponenten Kompetenz, Ehrlichkeit sowie Wohlwollen zusammensetzt (Casalo et al., 2008; Belanger et al., 2002; Lee & Turban, 2001; Urban et al., 2009), wie in Abbildung 21 grafisch dargestellt.

Abbildung 21: Vertrauenskomponenten (eigene Darstellung)

Kompetenz hängt mit der Wahrnehmung von Wissen und Fähigkeiten des Gegenübers zusammen und damit, ob ein Individuum glaubt, dass das Gegenüber in der Lage ist, seine Bedürfnisse zufriedenzustellen (Sitkin & Roth, 1993; Coulter & Coulter, 2002). **Ehrlichkeit** ist der Glaube, dass das Gegenüber sein Wort hält, seine Versprechungen erfüllt und aufrichtig ist (Doney & Cannon, 1997). **Wohlwollen** reflektiert den Glauben, dass die Parteien am Wohl der anderen Partei interessiert sind und nicht nur ihren eignen Profit maximieren wollen (Ganesan, 1994; Lee & Turban, 2001; Doney & Cannon, 1997).

Wirtschaftswissenschaftler argumentieren, dass Vertrauen jeweils situationsabhängig, informationsquellenabhängig und erfahrungsabhängig ist (Olson & Olson, 2000; Urban et al., 2009). In der wirtschaftswissenschaftlichen Vertrauensforschung können vier Kernelemente von Vertrauen identifiziert werden, (1) die Erwartungen,

(2) die Risikoübernahme, (3) der Kontrollverzicht sowie (4) die Zukunftsausrichtung (Abbildung 22).

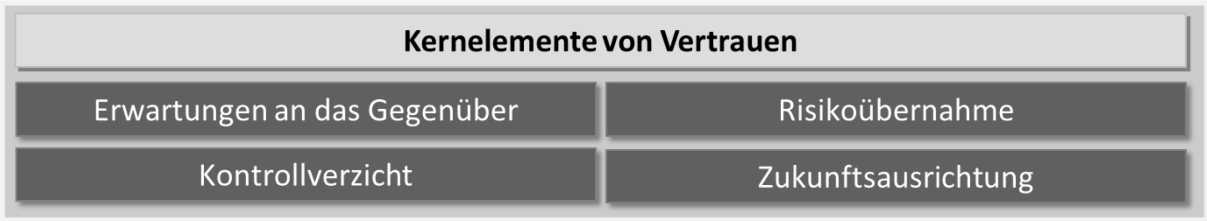


Abbildung 22: Kernelemente von Vertrauen (eigene Darstellung)

(1) Erwartungen an das Gegenüber: Cook und Wall (1980) umschreiben Vertrauen als das Ausmass, in dem jemand bereit ist, anderen Personen gute Absichten zuzuschreiben und damit ihren Worten und Handlungen zu vertrauen. Konkreter wird Rotter (1967) indem er sagt, dass Vertrauen auf der Erwartung einer Person oder einer Gruppe basiert, sich auf ein mündlich oder schriftlich gegebenes – positives oder negatives – Versprechen einer anderen Person bzw. Gruppe verlassen zu können. Vertrauen kann demnach als die Zuversicht beschrieben werden, dass das Gegenüber sein Versprechen halten wird (Sitkin & Roth, 1993).

(2) Risikoübernahme: Currall und Judge (1995) definieren Vertrauen als Umstand, bei dem sich ein Individuum bei der Wahl seines Verhaltens unter Eingehen eines Risikos auf eine andere Person verlässt. Vertrauen beinhaltet demnach die Inkaufnahme von Verletzlichkeit, indem man sich auf die Eigenschaften eines Objekts, das Eintreten eines Ereignisses oder das Verhalten einer Person verlässt, um in einer riskanten Situation ein gewünschtes, aber unsicheres Ziel zu erreichen (Griffin, 1967).

(3) Kontrollverzicht: Vertrauen beinhaltet, auf die Kontrolle des Gegenübers zu verzichten, ohne in der Lage zu sein, sich zu versichern, dass keine unvorteilhaften Konsequenzen daraus resultieren werden (Scanzoni, 1979; Morris & Moberg, 1994). Zündorf (1986) definiert Vertrauen als die freiwillige Übertragung der Kontrolle über Ressourcen, Handlungen oder Ereignisse in Erwartung einer nicht genau im Voraus festgelegten Gegenleistung in einer nicht genau terminierten Zukunft. Die Akzeptanz der Verletzlichkeit scheint ein sinnvoller Bestandteil einer Definition von Vertrauen, da dadurch andere Konstrukte wie Kooperation oder Vorhersagbarkeit ausgeschlossen werden. So verstehen auch Mayer, Davis und Schoorman (1995) unter Vertrauen: "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (S. 712).

(4) Zukunftsausrichtung: Vertrauen ist auf die zukünftigen Verhaltensweisen des Gegenübers gerichtet. Schlenker, Helm und Tedeschi (1973) verweisen darauf, dass sich Vertrauen immer auf zukünftige Handlungen anderer bezieht, die der eigenen Kontrolle entzogen sind und daher Ungewissheit und Risiko bergen. Vertrauen ist demnach auch der Glaube, dass der andere für einen irgendwann das tut, was man für ihn getan hat (Jackson, 1980).

Vertrauen als „Black Box" kann nicht aus einer rein wirtschaftlichen Perspektive betrachtet werden, sondern es müssen zusätzlich Sichtweisen aus Psychologie und Soziologie miteinbezogen werden. Der Grossteil der Beiträge von der psychologischen Seite stammt aus der Persönlichkeits- oder der Sozialpsychologie. Der Persönlichkeitspsychologe Rotter (1967) definiert Vertrauen als die Erwartung eines Individuums, dass man sich auf das Wort eines anderen Individuums oder einer Gruppe verlassen kann. Er argumentiert, dass Vertrauen erlernbar ist und dass Vertrauen ein Persönlichkeitsmerkmal darstellt. Der Sozialpsychologe Deutsch (1958) hat sein Verständnis von Vertrauen mithilfe des Gefangendilemmas[20] anhand des kooperativen Verhaltens abgeleitet. Deutsch (1958) versteht unter Vertrauen eine Erwartung an das Verhalten einer anderen Person, welche nicht der eigenen Kontrolle unterliegt, und in einer Situation, bei der der Schaden möglicherweise grösser sein könnte als der potenzielle Nutzen. Rousseau, Sitkin, Burt und Camerer (1998) definieren Vertrauen als "a psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or behaviors of another" (S. 395). Auch Siegrist, Gutscher und Earle (2005), definieren Vertrauen als "willingness to make oneself vulnerable to another based on a judgment of similarity of intentions or values" (S. 147). Mit diesen Definitionen betonen die Autoren, dass Vertrauen auf sozialen Beziehungen, Gruppenzugehörigkeit und geteilten Werten basiert.

Auch die soziologische Forschung betrachtet Vertrauen im Rahmen von sozialen Beziehungen. Nach Luhmann (1979; 2000) ist Vertrauen Konfidenz in die Erwartungen von Drittparteien und dient in erster Linie der Komplexitätsreduktion. Durch das Vertrauen klammert ein Mensch alle für ihn ungünstigen Verhaltensweisen der vertrauten Person aus und reduziert dadurch die Komplexität. Gemäss Brinkmann

[20] Das Gefangenendilemma ist ein Spiel mit zwei Personen, welche nicht miteinander kommunizieren können und sich entweder für Kooperation oder Verrat entscheiden können. Der Gewinn/Verlust beider Personen ist dabei eine Funktion der eigenen Verhaltensweise und derjenigen des Partners. Das Gefangenendilemma ist Bestandteil der Spieltheorie (Tucker & Kuhn, 1950).

und Seifert (2001) besteht Vertrauen aus drei Erwartungsdimensionen, welche an den Vertrauensempfänger gerichtet werden: Kompetenzerwartungen, Integritätserwartungen und Gesinnungserwartungen; dementsprechend definieren sie Vertrauen als „gefühlsmässige und/oder kalkulierte Bereitschaft eines Akteurs, auf die Kontrolle eines anderen zu verzichten und eine riskante Vorleistung zu erbringen, die meistens mit der kognitiven Erwartung und dem Gefühl einhergeht, dass der Vertrauensempfänger gleichzeitig kompetent, integer und wohlwollend ist“ (S. 27).

2.3.1.2 Vertrauensforschung im Internet

In der Literatur besteht Einigkeit darüber, dass Vertrauen im Internetkontext eine gesteigerte Bedeutung zukommt (Brinkmann & Seifert, 2001; Gefen & Straub, 2003). Wir haben gesehen, dass in der Offline-Welt Vertrauen als “a psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or behaviors of another” (Rousseau et al., 1998, S. 395) definiert wird. Das heisst, dass wir ein gewisses Mass an Verletzlichkeit in Bezug auf die Integrität und Seriosität des Gegenübers voraussetzen müssen, was auch bei Online-Transaktion der Fall ist. Bart, Shankar, Sultan und Urban (2005) wenden diese Definition auf den Online-Kontext an und unterstreichen dabei: “Online trust includes consumer perceptions of how the site would deliver on expectations, how believable the site’s information is, and how much confidence the site commands” (S. 134). Das Online-Vertrauen unterscheidet sich von weiteren Verständnissen von Vertrauen in der Offlinewelt nur darin, dass das Vertrauensobjekt eine Website darstellt – im Gegensatz zu Individuen, Gruppen, physischen Produkten oder Objekten etc. (Nissenbaum, 2001). Dies bedeutet, dass Online-Vertrauen immer dann generiert wird, wenn der Nutzer positive Eindrücke der Webpräsenz eines Transaktionspartners gesammelt hat und deshalb bereit ist, ein bestimmtes Mass möglicher Enttäuschungen in der Transaktion mit dem Geschäftspartner zu akzeptieren (Urban et al., 2009). Vertrauen gewinnt insbesondere dann an Bedeutung, wenn soziale Situationen von Risiko, Unsicherheit und wechselseitiger Abhängigkeit geprägt sind (Grabner-Kräuter & Kaluscha, 2003; McKnight & Chervany, 2002). In einer Online-Umwelt sind alle Transaktionen computergestützt und dies schränkt die Qualität und Quantität jener Hinweise ein, welche dem Konsumenten zur Beurteilung der Vertrauenswürdigkeit des Transaktionspartners zur Verfügung stehen (Friedman et al., 2000; Jarvenpaa et al., 2000; Yoon, 2002; Wang et al., 2004). Ein ganz wesentliches Element des Online-

Vertrauens ist die Bereitschaft, persönliche Daten mitzuteilen (Andrade, Kaltcheva & Weitz 2002; Jourard, 1971). Eine solche Mitteilung setzt aber den Nutzer einer gewissen Verwundbarkeit aus (Lanier & Saini, 2008). Zugleich ist sie jedoch eine notwendige Voraussetzung für die Durchführung einer Online-Transaktion (Scheonbachler & Gordon, 2002).

Operationalisierte Definition von Vertrauen: Von Vertrauen wird in dieser Dissertation gesprochen, wenn Nutzer bereit sind, dem Anbieter eines Online-Geschäftsmodells für eine versprochene Leistung persönliche Daten im Internet zu überlassen. Dies impliziert, dass von der Prämisse ausgegangen wird, dass mit der Höhe des Nutzervertrauens auch die Bereitschaft steigt, während einer Transaktion private Daten zur Verfügung zu stellen.

2.3.1.3 Die Bedeutung von Vertrauen für Anbieter von Online-Geschäftsmodellen

Fehlendes Vertrauen wird gemäss Urban et al. (2009) als die Barriere betrachtet, welche Nutzer von Online-Transaktionen abhält. In einer virtuellen Umgebung ist der Grad an Unsicherheit höher als bei traditionellen Transaktionsumgebungen (Grabner-Kräuter & Kaluscha, 2003). Vertrauen kann demnach als das Differenzierungsmerkmal bezeichnet und als zentraler Erfolgsfaktor von Online-Geschäftsmodellen angesehen werden (Cheskin, 1999; Gefen & Straub, 2003; Luo, 2002; Tan & Thoen, 2002; Grabner-Kräuter & Kaluscha, 2003). Vertrauen erfüllt sowohl im Privatleben als auch im Geschäftsleben mehrere Funktionen. Geschäftsbeziehungen werden durch Vertrauen erleichtert, da die Notwendigkeit extensiver Verhandlungen reduziert wird und die Transaktionskosten gesenkt werden können (Fukuyama, 1996; Dyer & Chu, 2003; Shapiro et al., 1992; Kramer, 1999). Weiter führt Vertrauen zu Komplexitätsreduktion, das heisst, es ermöglicht uns, mit der enormen Komplexität der sozialen Welt umzugehen, und für viele Menschen sind Internettransaktionen eine eher komplexe Angelegenheit (Riegelsberger & Sasse, 2001).

Da Nutzer und Anbieter zeitlich und örtlich getrennt auftreten, sind sie sich in der Regel völlig fremd und besitzen keine Erfahrungen bezüglich der Vertrauenswürdigkeit des anderen (Brinkmann & Seifert, 2001; Luo, 2002; Riegelsberger & Sasse, 2001; Gefen & Straub, 2003). Siegrist (2000) zeigt in seiner Studie auf, dass die Risikowahrnehmung einer Person mit steigendem Vertrauen abnimmt. Vertrauen steigert somit die Bereitschaft einer Person, risikoreiche Aktivitäten aufzunehmen, was einen positiven Effekt auf die Nutzung von Online-Geschäftsmodellen hat. Weiter

spielt Vertrauen bei der Adaption von neuen Technologien eine Schlüsselrolle und wird somit zu einer zentralen Vorbedingung von Online-Transaktionen (Brinkmann & Seifert, 2001; Gefen & Straub, 2003; Fukuyama, 1996).

Individuen sind je nach persönlichen Charakterzügen, Erfahrungen, demografischen Variablen oder psychologischen Merkmalen mehr oder weniger empfänglich für Vertrauen (Kotler et al., 2003). Das Vertrauen in einen Transaktionspartner ist darüber hinaus immer auch getragen vom Vertrauen in zugrunde liegende Institutionen, beispielswiese in das Internet als Medium oder in die relevanten Rahmenbedingungen (Sheehan & Hoy, 2000; McKnight et al., 1998; Lee & Turban, 2001; Walczuch & Lundgren, 2004). McKnight et al. (2002a) haben diese Faktoren in ihrem Web Trust Model zusammengeführt (Abbildung 23). Gemäss Dimitriadis & Kyrezis (2010) wird in 90 % der 65 wichtigsten Vertrauensartikel das Vertrauensmodell von McKnight et al. (2002a) verwendet. Diese drei Faktoren Vertrauensneigung, Vertrauen in die Institution und Vertrauen in den Anbieter sind interdependent (McKnight et al., 1998). Die Vertrauensneigung hat einen Einfluss auf das Vertrauen in die Institution Internet ebenso wie auf das Vertrauen in den Anbieter (McKnight et al., 2002a; 1998; Gefen, 2000). Im Folgenden werden die Komponenten des Web Trust Model von McKnight et al. (1998; 2002a) erläutert:

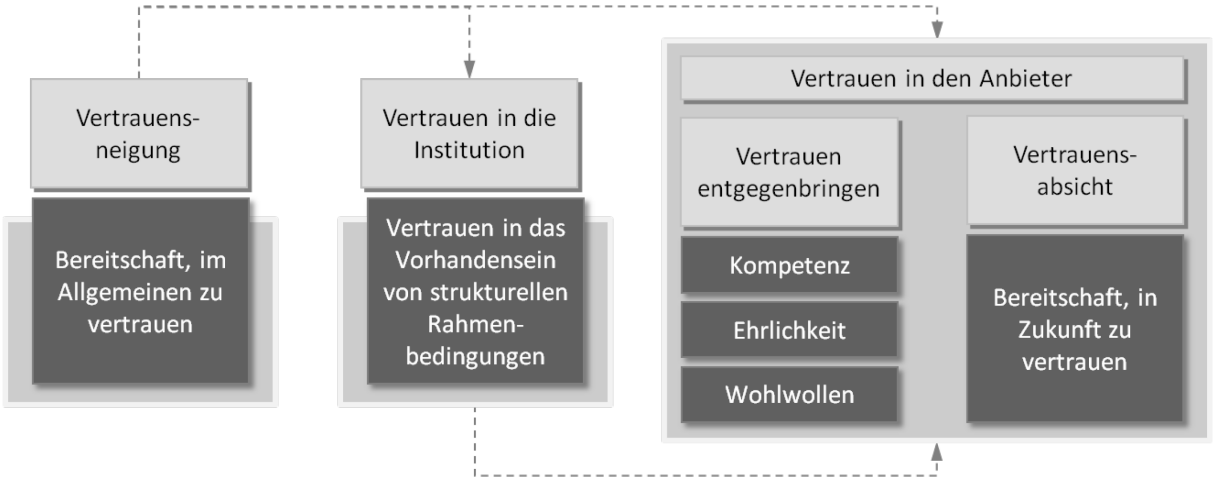


Abbildung 23: Web Trust Model (eigene Darstellung in Anlehnung an McKnight et al., 1998; 2002a)

Vertrauensneigung (Dispostition to Trust): Die Vertrauensneigung kann auch als generalisiertes Vertrauen bezeichnet werden, welches auf unterschiedliche Situationen anwendbar ist (Yamagishi & Yamagishi, 1994) und auf der Lebenserfahrung und der Sozialisation beruht (Gefen, 2000; Rotter, 1967). McKnight et al. (2002a) definieren: "Disposition to trust is the extent to which a person displays a tendency to be

willing to depend on others across a broad spectrum of situations and persons." (S. 339). Wu, Hu und Wu (2010) ergänzen: "(…) if someone has a high disposition to trust, he or she is more likely to believe in the goodness of human beings and is more willing to lend credit of trust for an initial interaction." (S. 8). Die Vertrauensneigung beeinflusst die Bereitschaft zu vertrauen, bevor Informationen über den Vertrauensnehmer (dies kann eine Person oder eine Institution sein) verfügbar sind (Mayer et al., 1995). Sie beinhaltet eine grundsätzliche Neigung respektive Abneigung gegenüber Vertrauen (Kramer, 1999) und ist eine stabile, situationsunabhängige Eigenschaft des Vertrauensgebers (Mayer et al., 1995). Deshalb wird die Vertrauensneigung nicht mehr als Zustand selbst, sondern als Persönlichkeitseigenschaft angesehen, in welcher sich Personen unterscheiden können (Rotter, 1980). Rotter (1980) stellt fest, dass vertrauensvolle Individuen einen Vertrauensvorschuss so lange gewähren, bis dieses Vertrauen verletzt wird, während misstrauische Individuen erst dann vertrauen, wenn der Vertrauensnehmer sich als des Vertrauens würdig erwiesen hat.

Vertrauen in die Institution (Institution-based Trust)[21]: McKnight et al. (2002a) definieren: "Institution-based trust is the belief that needed structural conditions are present (e. g., in the Internet) to enhance the probability of achieving a successful outcome in an endeavor like e-commerce." (S. 339). Das institutionsbasierte Vertrauen bezieht sich auf das Vertrauen gegenüber einer Institution, wie dies zum Beispiel das Internet ist. Für die zurückhaltende Nutzung von Online-Geschäftsmodellen kann mangelndes Vertrauen in das Internet verantwortlich gemacht werden (Pavlou & Gefen, 2004; Grabner-Kräuter & Kaluscha, 2003; Hoffman et al., 1999a; Egger, 2001). Nutzer haben unabhängig von einem Online-Anbieter eine grundsätzliche Einstellung gegenüber dem Internet und dessen Rahmenbedingungen, zum Beispiel in Bezug auf die Nützlichkeit, die Sicherheit, das Risiko usw. (Keen, Balance, Chan & Schrump, 1999; Egger, 2001). Gemäss Lee und Turban (2001) kommt es darauf an, ob der Nutzer die Prozesse versteht, welche das Internet steuern. Kim und Prabhakar (2002) konnten am Beispiel von Online-Banking nachweisen, dass nur Nutzer mit

[21] Eine Institution ist gemäss Duden (2013) einem bestimmten Bereich zugeordnete gesellschaftliche, staatliche oder kirchliche Einrichtung, die dem Wohl oder Nutzen des Einzelnen oder der Allgemeinheit dient. Das Internet kann als gesellschaftliche Einrichtung bezeichnet werden, welche ein Regelsystem mit eigenen Werten und Normen besitzt. Deshalb wird in dieser Arbeit das Internet als Institution bezeichnet.

Institutionsvertrauen bereit sind, sich für Online-Banking-Dienste registrieren zu lassen. Damit Offliner den Schritt ins Internet wagen und zu Nutzern werden, müssen sie dem Internet ein gewisses Mass an Vertrauen entgegenbringen. Lee und Turban (2001) explizieren in Bezug auf E-Commerce: "The extent to which consumers trust this computerized medium is likely to affect their overall trust in Internet shopping." (S. 80). Es wird von den Institutionen bzw. von ihren Vertretern erwartet, dass diese die Regeln und Normen überwachen und einhalten (Rousseau et al., 1998). Die wahrgenommene Zuverlässigkeit des Mediums hat demnach einen Einfluss auf die Nutzungsbereitschaft (McKnight et al., 2002a) und somit auf das Vertrauen in den Online-Anbieter, welches als Nächstes diskutiert wird.

Vertrauen in den Anbieter (Trust in Web Vendor): Das Vertrauen in den Anbieter setzt sich gemäss McKnight et al. (2002a) aus dem Vertrauensglauben (Trusting Beliefs) und den Vertrauensabsichten (Trusting Intention) zusammen. Dem Anbieter Vertrauen entgegenzubringen bezieht sich spezifisch auf die Wahrnehmung der Vertrauenswürdigkeit eines Anbieters: "Trusting beliefs means the confident truster perception that the trustee – in this context, a specific Web-based vendor – has attributes that are beneficial to the truster." (McKnight et al., 2002a, S. 337). Die Bereitschaft, einem Anbieter Vertrauen entgegenzubringen, setzt sich aus dem Glauben an die Komponenten Kompetenz, Ehrlichkeit sowie Wohlwollen zusammen (Casalo et al., 2008; Belanger et al., 2002; Lee & Turban, 2001; Urban et al., 2009), wie bereits bei der Definition von Vertrauen in Kapitel 2.3.1.1 festgestellt. McKnight et al. (2002a) diskutieren, dass der Vertrauensglaube und die Vertrauensabsichten das Vertrauen in den Anbieter definieren, aber auch, dass der Vertrauensglaube, und somit das Vertrauen in den Anbieter, zu positiven Vertrauensabsichten führten (ebenso testeten dies Schlosser et al., 2006)[22]. Auch diese Arbeit geht davon aus, dass zuerst Vertrauen in den Anbieter vorhanden sein muss, um eventuell in Zukunft dem Anbieter vertrauen zu können. Auf die Vertrauensabsichten wird später in dieser Arbeit in Kapitel 2.3.3.2 vertieft eingegangen. Die Items (Skalen) der Faktoren Vertrauensneigung, Vertrauen in die Institution und Vertrauen in den Anbieter aus dem Web Trust Model von McKnight et al. (1998; 2002a) wurden für die quantitative Online-Umfrage (siehe Methodik 3.1.2 und Anhang 7.4.1) übernommen.

[22] Die Arbeit von Grabner-Kräuter und Kaluscha (2003) widmet sich der Differenzierung der beiden Begriffe Trusting Beliefs und Trusing Intention. Die Autoren zeigen die Interpretation dieser beiden Begriffe in der Vertrauensforschungsliteratur anhand eines breit gefächerten Literaturüberblicks auf.

In diesem Kapitel wurde aufgezeigt, dass in der Vertrauensliteratur eine Vielzahl von Definitionen und Konzepten zu Vertrauen existieren. Trotz diesen ausführlichen theoretischen Modellen ist die individuelle Vertrauensneigung in der Realität schwer abzuschätzen, weil es nach wie vor so ist, dass Menschen unterschiedlich schnell und aus anderen Beweggründen heraus Vertrauen zu anderen Menschen oder Institutionen aufbauen. Individuen sind je nach kultureller Prägung, sozialem Status, persönlichen Lebensumständen oder psychologisch begründeten Einflüssen mehr oder weniger in der Lage zu vertrauen (Kotler et al., 2003). Die erste Forschungsfrage dieser Arbeit befasst sich deshalb damit, ob unterschiedliche Vertrauenstypen im Internet existieren:

Forschungsfrage 1: Existieren bei Internetnutzern unterschiedliche Vertrauenstypen?

Die Identifikation der Vertrauenstypen wird im Methodik-Kapitel 3.2.1 aufgrund der in diesem Kapitel vorgestellten Faktoren Vertrauen in den Anbieter, Vertrauensneigung sowie Vertrauen in die Institution vorgenommen. Wie auf das Vertrauen der Nutzer Einfluss genommen werden kann, wird im nächsten Kapitel behandelt.

2.3.2 Entstehung von Vertrauen

Dieses Kapitel geht der Frage nach, wie Vertrauen im Online-Umfeld entsteht und erzeugt werden kann. Das erste Kapitel 2.3.2.1 dient der Einführung in die Einflussfaktoren auf Vertrauen. Das zweite Kapitel 2.3.2.2 diskutiert die zentralen Einflussfaktoren im Online-Bereich und das dritte Kapitel 2.3.2.3 liefert einen tabellarischen Literaturüberblick über die besprochenen Vertrauensfaktoren.

2.3.2.1 Einführung in die Einflussfaktoren auf Vertrauen

Vertrauen entsteht in der Regel durch länger andauernde Interaktionen, also kontinuierlich (Hart & Saunders, 1997). Solche fortwährenden Interaktionen sind im Internetkontext indes nur selten anzutreffen. Die Einschätzung, ob eine Partei vertrau-

enswürdig ist oder nicht[23], stellt sich im Internet oft als schwierig heraus (Bhattacherjee, 2002). Die Transaktionspartner können anonym reagieren (Grabner-Kräuter & Kaluscha, 2003), die soziale Präsenz fehlt, die Beziehung ist zeit- und ortunabhängig und es handelt sich nicht um einen Simultanaustausch (Bhattacherjee, 2002; Gefen & Straub, 2003). Dies hat zur Konsequenz, dass die Transaktionspartner oft nur über wenig Information in Bezug auf die Vertrauenswürdigkeit der anderen Partei verfügen (Grabner-Kräuter & Kaluscha, 2003; Gefen, 2000). Es müssen demnach andere Wege gefunden werden, um Vertrauen im Internetkontext zu erzeugen.

In Anbetracht der enormen Bedeutung des Nutzervertrauens für Online-Transaktionen jeglicher Art stellt sich die Frage, welche Instrumente Online-Unternehmen einsetzen können, um das Vertrauen ihrer Nutzer zu gewinnen. Die Anzahl der Vertrauen beeinflussenden Faktoren in der Literatur ist extensiv, viele dieser Faktoren beziehen sich jedoch nicht nur auf den Online-Bereich. Im Internet beurteilen die Nutzer die Vertrauenswürdigkeit eines Transaktionspartners anhand von Hinweisen und Signalen, wobei es sich insbesondere um die Eigenschaften und Eindrücke des Online-Auftritts eines Anbieters handelt (Friedman et al., 2000; Jarvenpaa et al., 2000). Das Nutzervertrauen in der Webpräsenz eines Online-Unternehmens basiert auf den Merkmalen des Gewerbes selbst, den persönlichen Charakterzügen des Nutzers und dem Vertrauen des Nutzers in das gesamte Netzwerk der unterstützenden Institutionen (Jones et al., 2000; Nissenbaum, 2001; Sarathy & Robertson, 2003). In diesem komplexen Netzwerk von Faktoren, welche das Online-Vertrauen beeinflussen, können Online-Unternehmen die eigenen Merkmale und das äussere, von ihren Nutzern wahrgenommene Erscheinungsbild, meist direkt beeinflussen.

Die Betrachtung von Vertrauensfaktoren im Vertrauens-Management könnte wichtige Antworten dazu liefern, wie Vertrauen im Internet-Kontext erzeugt werden kann, und deshalb werden diese im folgenden Kapitel zusammengetragen, um sie zu einem konsistenten Bild der Vertrauenswürdigkeit eines Anbieters zusammenfügen.

[23] Misstrauen stellt nicht bloss das Gegenteil von Vertrauen dar. Misstrauen besteht, wenn eine Person eine Inkompatibilität zwischen ihren eigenen Überzeugungen und Werten sowie denen der Misstrauensperson wahrnimmt (Sitkin & Roth, 1993).

2.3.2.2 Zentrale Vertrauensfaktoren im Online-Bereich

In diesem Kapitel werden die zentralen Faktoren diskutiert, welche einen Einfluss auf die Vertrauensbildung der Nutzer im Online-Bereich haben (Abbildung 24). In der Vertrauensliteratur bestehen unzählige weitere Indikatoren, welche auf das Nutzervertrauen einwirken. In dieser Arbeit werden nur die zwölf meistgenannten Faktoren besprochen.

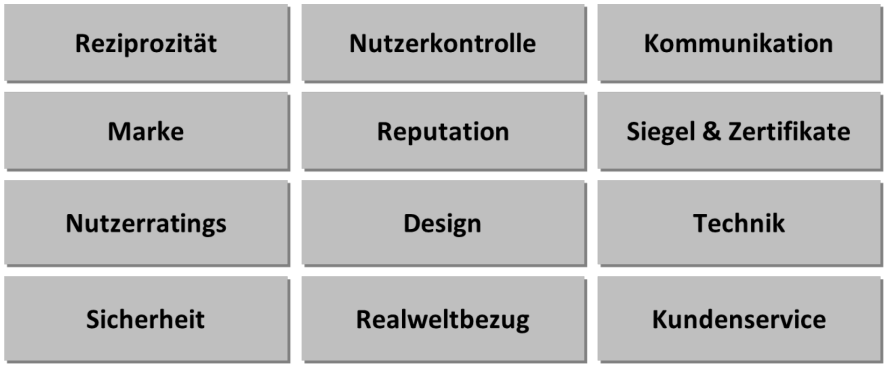


Abbildung 24: Relevante Vertrauensfaktoren (eigene Darstellung)

Reziprozität: Im Kapitel 2.1.2 wurde bereits diskutiert, dass heute aufgrund von technologischen Fortschritten Online-Unternehmen eine enorme Menge an Konsumentendaten effizient sammeln, aggregieren, analysieren und austauschen können, ohne dass die Nutzer dies wissen (Ashworth & Free, 2006; Chellappa & Sin, 2005; Glazer, 2001; Olivero & Lunt, 2004). Die Teilnahme an Online-Transaktionen setzt stets eine Preisgabe der Privacy der Nutzer voraus (Rust et al., 2002). Diese Entwicklung stellt Anbieter von Online-Geschäftsmodellen vor die Herausforderung, die Bereitschaft der Nutzer zu gewinnen, persönliche Daten für die Transaktion bereitzustellen (Chellappa & Sin, 2005). Die Entscheidung über diese Preisgabe fällt vor dem Hintergrund einer Abwägung des Umfangs erforderlicher Daten einerseits und erwarteter Nutzengewinne andererseits (Phelps et al., 2000; Homans, 1958; Chen & Barnes, 2007). Die Privacy-Calculus-Theorie besagt, dass die Transaktion nur dann durchgeführt wird, wenn der erwartete Nutzen einer Transaktion das empfundene Risiko durch die notwendige Preisgabe persönlicher Daten überschreitet (Krasnova et al., 2010; Olivero & Lunt, 2004). Der wahrgenommene Nutzen kann das Produkt oder die Dienstleistung selbst sein, aber ebenso die Orts- und Zeitunabhängigkeit, der Preis oder die Grösse der Auswahl (Bhatnagar et al., 2000; Anderson, 2007; Jarvenpaa & Tractinsky, 1999). Anbieter haben ihren Kunden die zu erwartenden Vorteile einer Transaktion und die Verhältnismässigkeit der erforderlichen Daten klar zu

kommunizieren (Ashworth & Free 2006; Olivero & Lunt, 2004). Ein fairer Grad an Reziprozität im Austausch von Daten, Geld, Produkten und Dienstleistungen kann helfen, Bedenken bezüglich der Privatsphäre oder die Risikowahrnehmung zu minimieren und Vertrauen aufzubauen (Sheehan & Hoy, 2000; Olivero & Lunt, 2004; Ashworth & Free, 2006; Phelps et al., 2000; Bhatnagar et al., 2000; Mayer et al., 1995).

Nutzerkontrolle: Haben sich Nutzer entschieden, an einer Transaktion im Internet teilzunehmen und persönliche Daten zur Verfügung zu stellen, geben sie aus ihrer Sicht nicht die Kontrolle über ihre eigenen Daten auf, sondern erwarten vom Anbieter, dass diese nicht über den von ihnen beabsichtigten Zweck hinaus verwendet werden. Viele Nutzer betrachten ihre Daten als Teil ihres Eigentums und dieses wird durch den Austausch in einer Online-Transaktion nicht völlig abgetreten (Sheehan & Hoy, 2000; Phelps et al., 2000; Olivero & Lunt, 2004). Um die Risikowahrnehmung der Nutzer zu senken und Vertrauen aufzubauen, ist es wichtig, dass die Kontrolle über die Daten stets beim Nutzer liegt (Bart et al., 2005; Culnan & Armstrong, 1999; Schoenbachler & Gordon, 2002). Viele Autoren sind der Auffassung, dass das Vertrauen in den Anbieter gesteigert werden kann, wenn der Nutzer die Kontrolle über seine Daten behält (Novak & Phelps, 1995; Hoffman & Novak, 2009; Urban et al., 2009). Sheehan und Hoy (2000) unterscheiden zwei Dimensionen der Nutzerkontrolle: „Awareness of information collection" bezieht sich auf das Bewusstsein des Nutzers über die Sammlung seiner Daten und „information usage" auf die Kenntnis der Verwendung der gesammelten Informationen. Anbieter müssen ihre Nutzer demnach darüber informieren, dass ihre Daten gesammelt werden, und dafür sorgen, dass Nutzer die Möglichkeit haben, ihre Daten eigenständig und selektiv zu verwalten, zum Beispiel durch Opt-out- und Opt-in-Funktionen (Milne & Rohm, 2000; Schoenbachler & Gordon, 2002). Ausserdem sollten Anbieter bei Weiterverwendung der Daten das Einverständnis beim Nutzer einholen (Culnan & Armstrong, 1999). Das Vertrauen der Nutzer dient dazu, die Wahrnehmung solcher Kontrollrisiken zu mildern.

Kommunikation: Nach Chadwick (2001) unterscheiden sich Online-Transaktionen von den Face-to-Face-Transaktionen dadurch, dass sich weniger schnell eine Beziehung entwickelt. Dies hat zur Folge, dass jegliche Information, welche zur Vereinfachung der Transaktion nötig ist, durch die Website bereitgestellt werden muss. Die Technologie bietet den Unternehmen jedoch heute eine breite Palette an Instrumenten, um den Nutzer online einzubinden und ihn mit Information zu versorgen. Unternehmen müssen von sich aus über die Privacy und die Sicherheit

der Nutzerdaten kommunizieren, denn proaktive Kommunikation der geplanten Datennutzung wird als vertrauenssteigernde Massnahme betrachtet (Chadwick, 2001; Geyskens, Steenkamp & Kumar, 1998; Lewicki & Bunker, 1995; Morgan & Hunt, 1994; Speier, Harvey & Palmer, 1998), wenngleich eine solche Kommunikationspolitik durch eine Steigerung der Aufmerksamkeit auch Vorbehalte und Sorgen auf Nutzerseite erhöhen kann (Milne & Boza, 1999; Sheehan & Hoy, 1999). Webseiten bieten dem Nutzer zahlreiche Möglichkeiten, um Fragen zu stellen, Komplimente oder Reklamationen zu äussern, was sich wiederum auf die Drittparteiempfehlungen auswirkt. Zudem dienen Chats, Foren oder Blogs dazu, die Konsumenten mit neuen und relevanten Informationen bezüglich der Sicherheits- und Privacyrichtlinien sowie der Kundendienstleistungen zu versorgen (Hart & Blackshaw, 2005). Unternehmen können Online-Communitys erschaffen, in welchen die Nutzer einerseits miteinander diskutieren können, andererseits aber mit dem Unternehmen selbst in Kontakt treten können (Casalo et al., 2008; Urban, Sultan & Qualls, 2000). Dabei ist es elementar, dass der Anbieter stets transparent, fair und auf gleicher Augenhöhe mit dem Nutzer kommuniziert.

Marke: Zahlreiche Studien befassen sich mit dem Einfluss von Marken auf die Entscheidungsfindung bei Online-Transaktionen (Bart et al., 2005; Corbitt, Thanasankit & Yi, 2003; Ha & Perks, 2005; Jevons & Gabbott, 2000). Der Anbieter muss glaubhaft darstellen können, dass er die Fähigkeit besitzt, Produkte oder Dienstleistungen zuverlässig und in der erwarteten Qualität liefern zu können (Palmer, Bailey & Faraj, 2000). Nutzer sind eher bereit, ihr Vertrauen grossen und bekannten Marken mit einem hohen Marktanteil zu schenken (Urban et al., 2000; Aaker, 1995; 2000; Berry, 2000; Doney & Cannon, 1997; Krishnamurthy, 2001; Luo & Cook, 2007–2008): "A perception of a large organization size implies that the merchant has significant resources invested in the business and has much to lose by acting in an untrustworthy way. Hence, the larger the firm, the more it is perceived by customers that it is in the firm's best interest to fulfill its promises to the consumer." (Jarvenpaa & Tractinsky, 1999, S. 29). Starke und bekannte Marken sind im Netz meistens gut vernetzt und deshalb wird die prominente Listung bei Suchmaschinen als vertrauenswürdiges Indiz wahrgenommen (Sen, 2005). Die Suchmaschinenoptimierung (auch Search En-

gine Optimization, SEO genannt)[24] ist demnach ein weiteres Instrument für Online-Anbieter, Vertrauen zu generieren.

Reputation: Neben der Marke spielt jedoch auch die Sympathie und die Reputation des Unternehmens eine zentrale Rolle bei der Risikowahrnehmung (Luo & Cook, 2007–2008). Eine gute Reputation schafft bei den Nutzern im Offline- (Doney & Cannon, 1997) wie auch im Online-Bereich (Jarvenpaa & Tractinsky, 1999) Vertrauen: "The status of a brand is based on its reputation. A good reputation creates trust, and trust earns loyalty." (Fraser & Dutta, 2009, S. 181). Sandberg (2002) definiert die Reputation einer Firma als "the consensus of perceptions about how a firm will behave in any given situation" (S. 3). Nutzervertrauen basiert vor allem auf einem entsprechenden Reputationsvorsprung des Anbieters, der zum Beispiel aus einer bekannten, sympathischen Marke hervorgeht (Jarvenpaa et al., 2000; Corbitt et al., 2003; Ha & Perks, 2005; Jevons & Gabbott, 2000; Walczuch & Lundgren, 2004; Eastlick et al., 2006; McKnight et al., 2002b). Wo ein solcher Reputationsvorsprung noch nicht etabliert werden konnte, empfiehlt sich die Kooperation mit etablierten Anbietern und Drittparteien. Die Reputation eines Unternehmens ist ein strategischer Wert und baut sich über einen längeren Zeitraum hinweg auf: Es sind Erlebnisse, Gefühle, Erfahrungen, Eindrücke und Wissen, die Menschen aus der Interaktion mit dem Unternehmen gewinnen und zu einem Gesamteindruck verdichten (Bauhofer, 2004; Xie et al., 2006). Deshalb kann davon ausgegangen werden, dass das Unternehmen diesen Wert nicht leichtfertig aufs Spiel setzt – dies macht zukünftiges Verhalten absehbarer und reduziert bei den Internetnutzern Unsicherheit (Xie et al., 2006). Die Reputation einer Firma ist somit ein wichtiger Faktor, um Kundenvertrauen zu schaffen (Chen & Barnes, 2007; Marwick et al., 2010; Xie et. al., 2006; Koufaris & Hampton-Sosa, 2004).

Siegel und Zertifikate: Mehrere Studien weisen nach, dass Programme von Drittparteien das Konsumentenvertrauen und ihre Transaktionsabsichten beeinflussen

[24] Suchmaschinen sind zum Beispiel Google, Bing, Yahoo, MSN oder Ask. Optimierung bedeutet, bei einem entsprechenden Suchbegriff in den unbezahlten Rankings möglichst weit oben zu erscheinen, um die Visibilität des Unternehmens und seinen Bekanntheitsgrad zu erhöhen. Google ist zurzeit die meist genutzte Suchmaschine, wer nicht bei Google erscheint, existiert nicht. Google verwendet das Verfahren des PageRank-Algorithmus, benannt nach dessen Entwicklern Larry Page und Sergei Brin. Jedem Dokument oder jeder Internetseite wird aufgrund seiner Verlinkungsstruktur ein PageRank zugeordnet und je höher dieser ist, desto höher erscheint die Seite in der Suchmaschine. Je vernetzter eine Seite ist (je mehr Links auf die Seite verweisen), desto beliebter ist die Seite und desto höher der PageRank und somit die Listung bei Google (Alby & Karzauninkat, 2007; Winkler, 2007).

können (Wakefield & Whitten, 2006; Cheskin/Sapient, 1999; McKnight & Chervany, 2002; McKnight, Choudhury & Kacmar, 2000; Palmer et al., 2000; Riegelsberger & Sasse, 2001; Shneiderman, 2000; Urban et al., 2000; Hu, Wu, Wu & Zhang, 2010). Die Bekräftigung durch Drittparteien ermöglicht es den Nutzern, auf einen Blick zu beurteilen, ob ein Online-Anbieter vertrauenswürdig ist oder nicht (Wang et al., 2004; Smith, Menon & Sivakumar, 2005); Drittparteien fungieren somit als Mittler zwischen den konkurrierenden Online-Anbietern und den Nutzern (Cook & Luo, 2003). Heutzutage existiert eine breite Palette von Vertrauenszertifikaten und Gütesiegeln, welche von unterschiedlichen Organisationen angeboten werden, dazu gehören beispielsweise VeriSign, Stiftung Warentest oder Consumer Reports (Cook & Luo, 2003; Krishnamurthy, 2001; McKnight et al., 2000; Palmer et al., 2000), wie in Abbildung 25 dargestellt. Diese Siegel oder Zertifikate können qualitätsbezogen (z. B. Ktipp), prozessbezogen (z. B. ISO-Zertifizierung), ökologiebezogen (z. B. Öko-Tex), handelsbezogen (z. B. Max Havelaar), servicebezogen (z. B. TÜV Service Tested) oder sicherheitsbezogen (z. B. VeriSign) usw. sein.

Abbildung 25: Beispiele von Vertrauenszertifikaten (eigene Darstellung)

Diese unabhängigen Stellen verleihen bei Bestehen der Sicherheitsprüfung Gütesiegel oder Zertifikate, welche Vertrauenswürdigkeit und Sicherheit demonstrieren sollen (Cook & Luo 2003; Palmer et al., 2000). Die prominente Platzierung solcher Zertifikate und Empfehlungen auf der Website sowie deren aktive Integration in die Kommunikationsaktivitäten der Anbieter sind inzwischen gängige Geschäftspraxis (Eastlick et al., 2006).

Nutzerratings: Online-Anbieter setzen aber auch auf die Wirkung von Ratings, Kommentaren und Berichten von Nutzern (Smith et al., 2005; Pennington, Wilcox & Grover, 2003). Mundpropaganda erzeugt einen komparativen Vorteil durch Wohlwollen und Glaubwürdigkeit (Pavlou, 2002) oder wie Friedman et al. (2000) betonen: "People trust people, not technology." (S. 36). Einem einzelnen Unternehmen oder einem Fremden glaubt man nicht, einer Gruppe von Menschen aber schon viel eher.

Kimmel (2010) weist darauf hin, dass Menschen das Bedürfnis haben, ihre Erfahrungen mit Produkten oder Unternehmen an Dritte weiterzugeben, besonders, wenn diese sehr gut oder sehr schlecht waren (s. a. Smith et al., 2005). Technisch einfach durchzuführen ist zum Beispiel die Verlinkung mit dem Facebook-„Like"-Button. Brinkmann & Seifert (2001) konnten nachweisen, dass sich bei schlechten Bewertungen auch die Anzahl der Transaktionen verringert. Online-Anbieter können das Konzept der Meinungsführer heranziehen. Meinungsführer sind Personen, welche sich zu einem bestimmten Thema oft äussern und mit dieser Äusserung andere Menschen beeinflussen können (Dressler & Telle, 2009). Meinungsführer können sich in der realen (z. B. Sportler, engagierte Konsumenten, Superstars) und in der virtuellen Welt (A-Blogger[25], Community-Teilnehmer) etablieren. Sie gelten als glaubwürdige Informationsquellen, da sie als neutral und objektiv wahrgenommen werden. Online-Anbieter sollten versuchen, Meinungsführer in ihrer Branche zu identifizieren und diese für sich zu gewinnen, denn diese können die Zielgruppe mit Informationen über das Produkt oder die Marke in ihrer Entscheidungsfindung beeinflussen (Huber, 2008; Pleil, 2005).

Design: Online-Anbieter sollten vor allem Wert auf eine nutzerfreundliche und leistungsfähige Benutzeroberfläche legen, welche Bequemlichkeit im Umgang und in der Navigation verbindet (Schlosser et al., 2006; Cheskin/Sapient, 1999; Riegelsberger & Sasse, 2001; Gefen & Straub, 2003). Denn bereits der erste Eindruck, welcher ein Nutzer von der Website hat, kann für die Bildung von Vertrauen entscheidend sein (Egger, 2000; 2001; Kim & Moon, 1998; McKnight et al., 2002b). Shneiderman (2000) stellt fest: "good design can inspire trust" (S. 59). Die Qualität der Benutzeroberfläche bietet dem Nutzer massgebliche Hinweise zur Qualität des Angebots und auf die Fähigkeit, ob die versprochene Leistung erfüllt werden kann. Insbesondere für erfahrene Nutzer ist das Design einer Homepage das wichtigste Indiz für oder gegen eine Transaktionsentscheidung bei einem Anbieter (Riegelsberger & Sasse, 2001). Deshalb

[25] A-Blogger geniessen über ihren Blog eine sehr hohe Aufmerksamkeit und weisen ein dichtes, stabiles Netzwerk auf. Oft sind sie Journalisten oder Berater, welche die Kommunikationsmechanismen kennen und gewohnt sind, auf die Meinungsbildung Einfluss zu nehmen (Pleil, 2005). Zu Meinungsmacher-Blogs zählen Weblogs, die mit mehr als 100 anderen Blogs verlinkt sind (Huber, 2008). Klassische Massenmedien greifen für ihre Berichterstattung gerne Themen auf, die in Meinungsführer-Blogs behandelt werden und diese werden so wiederum einem noch breiteren Kreis von Lesern zur Verfügung gestellt (Pleil, 2005).

argumentieren Chau, Au und Tam (2000), dass die Hauptherausforderung eines Online-Anbieters darin liegt, eine benutzerfreundliche und leistungsfähige Oberfläche zu entwerfen. Einfachheit, Verständlichkeit, Korrektheit, Aktualität und Qualität der Inhalte einer Website sind wichtige Faktoren eines vertrauenerweckenden Designs (Nielsen, 1999; Urban et al., 2000; Belanger et al., 2002; Corbitt et al., 2003). Das Design muss die Professionalität unterstreichen und der Übersichtlichkeit dienen, damit Funktionalität und Navigation möglichst nutzerfreundlich sind (Cheskin/Sapient, 1999; Shneiderman, 2000; Krishnamurthy, 2001; Riegelsberger & Sasse, 2001; Gefen & Straub, 2003). Die Nutzerfreundlichkeit bezieht sich auf die wahrgenommene Einfachheit der Bedienung einer Homepage und beeinflusst das Vertrauen des Nutzers in den Anbieter (Riegelsberger & Sasse, 2001; Koufaris & Hampton- Sosa, 2004; Gefen & Straub, 2003; Nielsen, 1999). Nutzer haben ein klares Verständnis dafür entwickelt, wie die Website eines Online-Händlers, eines sozialen Netzwerks oder einer Online-Bank auszusehen und zu funktionieren hat. Jegliche Funktionalitäten, welche diesen erlernten Schemata folgen oder den Nutzer durch den Entscheidungsfindungsprozess begleiten, vereinfachen die Interaktion mit dem Anbieter (Fang & Salvendy, 2003; Gefen, 2000; Gefen, Karahanna & Straub, 2003). Anbieter von Online-Geschäftsmodellen sollten daher vertraute Elemente und Prozesse integrieren und durch Aktionsbestätigungen, Prozessfeedbacks und konstruktive Fehlermeldungen helfen, dem Nutzer das Gefühl zu verleihen, das System kontrollieren zu können (Egger, 2001; Yoon, 2002). Alle auf der Website positionierten Angaben wie Bilder, Produktpräsentationen, Farben oder Schriftarten vermitteln dem Nutzer Hinweise über die Vertrauenswürdigkeit des Anbieters (Chau et al., 2000; Riegelsberger, Sasse & McCarthy, 2003).

Technik: Der Zuverlässigkeit der technischen Infrastruktur im Internet kommt eine besondere Bedeutung zu (Lee & Turban, 2001; Corbitt et al., 2003). Wie bereits bei dem Vertrauen in die Institution thematisiert, beeinflusst das Vertrauen, welches der Nutzer dem Internet als Medium entgegenbringt, das Vertrauen in Online-Unternehmen an sich (Egger, 2001; Lee & Turban, 2001). Der Nutzer muss sich während einer Transaktion auf die technische Infrastruktur des Systems verlassen können und dafür muss er von der technischen Kompetenz des Anbieters überzeugt sein (Gefen & Straub, 2003). Lee und Turban (2001) definieren die technische Kompetenz des Systems als die Fähigkeit, Aufgaben gemäss ihren Voraussetzungen auszuführen. Nielsen (1999) beschreibt die Auswirkung einer kompetenten Technologie auf das Vertrauen: “Appropriate use of technology from encryption to download speed

also matters: users feel that a professionally run server can be trusted more than one that feels like it could break at any time" (o. S.). Anhaltspunkte für technische Kompetenz von Unternehmen sind Faktoren wie Schnelligkeit, Navigation, Verfügbarkeit, Sicherheit sowie Auftragserfüllung (Lee & Turban, 2001; Bart et al., 2005; Hoffmann, Novak & Peralta, 1999a; Johnson, 2007). Die Bedeutung des Vertrauens wird durch das meist nur vage Verständnis des Konsumenten von der technischen Architektur sowie der Arbeitsweise des Internets noch verstärkt (Johnson, 2007). Umgekehrt haben Störungen, Defekte sowie Tippfehler auf einer Homepage einen negativen Einfluss auf das Vertrauen der Nutzer (Urban et al., 2009; Nielsen, 1999; Fang & Salvendy, 2003).

Sicherheit: Die vom Nutzer wahrgenommene Sicherheit einer Website hat einen positiven Einfluss auf dessen Vertrauen (Chen & Barnes, 2007; McKnight & Chervany, 2002; Palmer et al., 2000; Ratnasingam, 1998; Riegelsberger & Sasse, 2001; Urban et al., 2000). Lücken im Sicherheitssystem steigern die Wahrscheinlichkeit von Manipulationen oder Diebstählen. Um dem Bedürfnis nach Sicherheit nachzukommen, wurde in den letzten Jahren viel in Sicherheitsmassnahmen investiert, zum Beispiel in Zugangskontrollen (Firewalls), digitale Unterschriften, digitale Zertifikate, Verschlüsselungen, Applikationsprotokolle, verbesserte Zahlungssysteme etc. (Belanger, et al., 2002; Ratnasingam, 1998; Riegelsberger & Sasse, 2001). Die adäquate Pflege von Infrastruktur, Software und Prozessen sowie effektive Managementprozesse schützen und erhöhen die Sicherheit der Beteiligten (Belanger et al., 2002; Nissenbaum, 2001; Koufaris & Hampton-Sosa, 2004). Aufgrund der vertrauensfördernden Wirkung solcher Sicherheitsmassnahmen müssen diese dem Kunden auch proaktiv kommuniziert werden und auf der Seite muss klar ersichtlich sein, über welche Sicherheitsinfrastrukturen sie verfügt (Hu et al., 2010).

Realweltbezug: Ein Unternehmen, welches auch physisch existiert, hat beim Aufbau von Vertrauen Vorteile. Unternehmen, welche sich in der Offline-Welt etabliert haben, werden auch im Online-Bereich als „realer" wahrgenommen (Olivero & Lunt, 2004), da die Offline-Präsenz dem Konsumenten enorm viele Anhaltspunkte bereitstellt, welche eine Vertrauensbildung ermöglichen (Friedman et al., 2000). Auch Online-Anbieter können durch einen „Realweltbezug" Vertrauen erzeugen (Jarvenpaa & Tractinsky, 1999; Gefen & Straub, 2003). Die Kommunikation eines Realweltbezuges kann einfache Elemente wie die Benennung der Verantwortlichen des Unternehmens, das Zeigen von Bildern der Verantwortlichen sowie die umfassende Angabe von Kontaktmöglichkeiten beinhalten (Jarvenpaa & Tractinsky, 1999). Viele

Anbieter, welche fast ausschliesslich im virtuellen Geschäft tätig sind, versuchen bereits, Elemente innerhalb ihrer Website zu integrieren, welche auf eine Offline-Präsenz hinweisen, indem zum Beispiel Bilder der Hauptniederlassung oder von Mitarbeitern gezeigt werden (Zimmer, 2010).

Kundenservice: Urban et al. (2000) sehen die Vertragserfüllung als Haupttreiber des Online-Vertrauens. Die Fähigkeit einer Firma, die versprochene Ware zur richtigen Zeit am richtigen Ort zu liefern oder Expertenwissen zu besitzen und zu vermitteln, ist ein wichtiges Indiz für die Vertrauenswürdigkeit eines Anbieters (Fassnacht & Köse, 2007; Brinkmann & Seifert, 2001; Mayer et al., 1995; Deutsch, 1958; Sitkin & Roth, 1993; Ha & Perks, 2005). Eine faire Behandlung des Nutzers und eine Erfüllung der versprochenen Leistung wirkt sich positiv auf die Kundenzufriedenheit und somit das Vertrauen aus (Clemmer & Schneider, 1996; Sheehan & Hoy, 1999; Culnan & Armstrong, 1999). Tadelloser, freundlicher und schneller Kundenservice kann, auch wenn die Kundenerwartungen hinsichtlich Qualität der Dienstleistung oder der Produkte des Anbieters nicht erfüllt werden, verlorenes oder angeschlagenes Vertrauen wiederherstellen (Schoenbachler & Gorden, 2002; Culnan & Armstrong, 1999; Harris & Goode, 2004; Shankar, Smith & Rangaswamy, 2003; Yen & Gwinner, 2003; Yoon, 2002). Der Nutzer weiss, dass er über die Homepage mit einem automatisierten System interagiert und deshalb werden auch einige automatisierte Kundenservice-Funktionen toleriert oder erwartet, zum Beispiel ausführliche „Frequently Asked Questions“ (FAQ), automatisierte Antworten oder das Tracking der Lieferung (Pavlou & Gefen, 2004). Urban et al. (2000) empfehlen den Einsatz eines Avatars als virtuellen Berater, welcher die gewünschte Information bereitstellt. Daneben müssen aber weitere Möglichkeiten zur Kontaktaufnahme, zum Beispiel per Callcenter oder per E-Mail, zur Verfügung stehen (Timmers, 2000; Fang & Salvendy, 2003).

Die Items der einzelnen Faktoren wurden aus der Literaturrecherche für die quantitative Online-Umfrage übernommen und durch die qualitative Voruntersuchung sowie den Pretest angepasst (siehe dazu auch Methodik-Kapitel 3.1.2 und Fragebogen im Anhang 7.4.1).

2.3.2.3 Literaturüberblick über die zentralen Vertrauensfaktoren

In Tabelle 1 sind die wichtigsten in der Literatur genannten Einflussfaktoren auf die Vertrauensbildung im Online-Bereich zusammengestellt, wobei die Liste nicht als abschliessend zu betrachten ist.

Autoren (Jahr)	Fokus des Papers	Vertrauensfaktoren
Bart, Shankar, Sultan & Urban (2005)	Charakteristika der Nutzer wie auch die der Seite beeinflussen das Vertrauen der Nutzer, welches das Verhalten im Internet beeinflusst. Die Effekte von Vertrauen unterscheiden sich zwischen Seiten und Konsumentengruppen.	Design Kundenservice Marke Sicherheit Technik
Belanger, Hiller & Smith (2002)	Analyse der Vertrauensfaktoren, welche beim E-Commerce Bedenken bezüglich der Privacy reduzieren.	Design Nutzerkontrolle Sicherheit Siegel & Zertifikate
Bhatnagar, Misra & Rao (2000)	Das Paper untersucht die Sicherheit bei Internetverbindungen. Limitierte Produktrisiken reduzieren die Risikowahrnehmung.	Kundenservice Reziprozität Technologie
Brinkmann & Seifert (2001)	Das Paper untersucht die Rolle von Vertrauen bei E-Commerce-Transaktionen und wie Vertrauen gefördert werden kann.	Kundenservice Nutzerratings
Chellappa & Sin (2005)	Das Paper untersucht das Dilemma zwischen Personalisierung und Privacy.	Reziprozität
Chen & Barnes (2007)	Das Paper untersucht das Kundenverhalten anhand von Vertrauensfaktoren beim E-Commerce.	Reputation Reziprozität Sicherheit
Cheskin/Sapient (1999)	Umfassende Studie zu Vertrauen beim Online-Shopping.	Design Kundenservice Marke Siegel & Zertifikate Technologie
Cook & Luo (2003)	Empfehlungen wie Gütesiegel oder Zertifikate sind Mittler zwischen den kompetitiven Online-Anbietern und den nervösen Online-Kunden.	Siegel & Zertifikate
Corbitt, Thanasankit & Yi (2003)	Schlagen ein Modell mit Vertrauensfaktoren im B2C-Bereich vor.	Design Erfahrung Marke Reputation Technologie
Culnan & Armstrong (1999)	Die Wahrnehmung von fairen Prozessen, welche die Privacy der Nutzer schützen, fördert die Bereitschaft, persönliche Informationen zur Verfügung zu stellen.	Kommunikation Kundenservice Nutzerkontrolle Technologie
Eastlick, Lotz & Warrington (2006)	Bestätigt die positive Beziehung zwischen der Reputation einer Firma und dem Vertrauen in E-Commerce. Privacybedenken haben einen negativen Einfluss auf die Kaufabsicht.	Nutzerkontrolle Reputation Sicherheit
Fassnacht & Köse (2007)	Der Kundenservice beeinflusst die Nutzerzufriedenheit, das Vertrauen, die Vertrauensabsichten und die Kaufabsichten.	Kundenservice
Gefen & Straub (2003)	Wahrgenommener Realweltbezug fördert das Vertrauen in den Online-Anbieter.	Design Kundenservice Realweltbezug
Gefen (2000)	Vertrautheit mit dem Online-Anbieter und dessen Prozessen fördert Vertrauen und beeinflusst das Kaufverhalten.	Design Vertrautheit

Ha & Perks (2005)	Das Paper identifiziert Erfahrung mit der Marke, Vertrautheit und Kundenzufriedenheit als Treiber von Vertrauen.	Kundenservice Marke Vertrautheit
Hu, Wu, Wu & Zhnag (2010)	Das Paper untersucht den Einfluss von Siegeln und Zertifikaten auf Vertrauen.	Sicherheit Siegel & Zertifikate
Jarvenpaa, Tractinsky & Vitale (2000)	Grösse und Reputation eines Online-Anbieters beeinflusst die Risikowahrnehmung und die Kaufbereitschaft.	Marke Reputation
Jevons & Gabbott (2000)	Das Paper untersucht den Zusammenhang zwischen Vertrauen und Marken bei Geschäftsbeziehungen im Internet.	Marke
Johnson (2007)	Das Paper untersucht den Zusammenhang zwischen Vertrauen und Technologie im Internet.	Technik
Koufaris & Hampton-Sosa (2004)	Das Paper untersucht den Zusammenhang von Reputation, Design, Kontrolle und Sicherheit auf das Vertrauen bei neuen Kunden im Internet.	Design Nutzerkontrolle Reputation Sicherheit
Lee & Turban (2001)	Das Paper untersucht ein theoretisches Modell mit Faktoren, welche das Vertrauen von Konsumenten beim Internetshopping beeinflussen.	Kundenservice Sicherheit Siegel & Zertifikate Technologie
Luo & Cook (2007-2008)	Das Paper identifiziert die wahrgenommene Reputation, Ehrlichkeit und Kompetenz als vertrauensrelevant bei Rating-Services im Internet. Der Effekt wird durch die Vertrauensneigung beeinflusst.	Kundenservice Marke Reputation Siegel & Zertifikate
McKnight, Choudhury & Kacmar (2002b)	Das Paper untersucht ein Vertrauensmodell im E-Commerce, welches neben den Vertrauensfaktoren auch die Vertrauensneigung, Vertrauen in die Institution, Vertrauensglauben und Vertrauensabsichten beinhaltet.	Design Reputation
Olivero & Lunt (2004)	Untersuchen die Rolle von Vertrauen bei Privacybedenken und der Bereitstellung von persönlichen Daten.	Nutzerkontrolle Realweltbezug Reziprozität
Phelps, Novak & Ferrell (2000)	Das Paper untersucht die Beziehung zwischen Privacybedenken und der Bereitstellung von persönlichen Daten.	Nutzerkontrolle Reziprozität
Riegelsberger & Sasse (2001)	Das Paper untersucht ein Modell mit vertrauensfördernden und vertrauenszerstörenden Faktoren im E-Commerce.	Design Marke Reputation Sicherheit
Schlosser, White & Lloyd (2006)	Das Paper untersucht, ob das Design einer Seite einen positiven Effekt auf das Vertrauen und die Kaufabsicht hat.	Design
Smith, Menon & Sivakumar (2005)	Das Paper untersucht den Einfluss von Empfehlungen auf die Entscheidungsfindung beim Online-Shopping.	Nutzerratings Siegel & Zertifikate
Urban, Sultan & Qualls (2000)	Die Autoren betonen die Wichtigkeit von Vertrauensfaktoren für Online-Geschäftsmodelle und schlagen Instrumente zur Vertrauensbildung vor, wie zum Beispiel virtuelle Berater.	Design Kommunikation Kundenservice Marke Sicherheit Siegel & Zertifikate Technik
Yen & Gwinner (2003)	Konzeptionelles Modell, welches den Einfluss von wahrgenommen Vorteilen auf Loyalität und Kundenzufriedenheit untersucht.	Kundenservice Nutzerkontrolle
Yoon (2002)	Entwickelt ein Modell mit Vertrauensfaktoren beim E-Shopping.	Design Kundenservice Reputation

Tabelle 1: Literaturüberblick über die zentralen Vertrauensfaktoren

Sehr viele Studien haben sich in den vergangenen Jahren mit den Einflussfaktoren auf Vertrauen im Online-Bereich befasst, wie in Tabelle 1 ersichtlich wird. Auf die Frage jedoch, ob diese Vertrauensfaktoren von verschiedenen Personengruppen unterschiedlich wahrgenommen werden, konnten diese Studien keine Auskunft geben. Deshalb widmet sich die zweite Forschungsfrage dieser Dissertation der folgenden Thematik:

Forschungsfrage 2: Sind während einer Transaktion im Internet für die unterschiedlichen Vertrauenstypen dieselben Vertrauensfaktoren relevant?

Die in Abbildung 24 gezeigten, im Rahmen der Literaturrecherche identifizierten zwölf Faktoren werden durch qualitative Interviews mit Anbietern und Nutzern vertieft betrachtet und es wird darauf geachtet, wie die Interviewteilnehmer die Faktoren beschreiben und verstehen. Die Identifikation der unterschiedlichen Vertrauensfaktoren pro Vertrauenstyp wird im Methodik-Kapitel 3.2.1 aufgrund der vorgestellten Vertrauensfaktoren vorgenommen. Im folgenden Kapitel wird das Vertrauen als dynamischer Prozess, als Ergebnis von Transaktionen, näher betrachtet.

2.3.3 Vertrauen als Ergebnis

Im vorhergehenden Kapitel 2.3.1.3 wurde bereits erwähnt, dass Vertrauen in den Anbieter zu positiven Vertrauensabsichten führen kann (McKnight et al., 2002a; Schlosser et al., 2006). Dieses Kapitel betrachtet das Nutzervertrauen als dynamischen Prozess (Kapitel 2.3.3.1) und untersucht, inwiefern Vertrauen als Resultat (Kapitel 2.3.3.2) betrachtet werden kann.

2.3.3.1 Vertrauen als dynamischer Prozess

Insbesondere Wirtschaftswissenschaftler betrachten in ihrer Forschung vermehrt Momentaufnahmen oder statische Phänomene, da diese präziser und kontrollierter beschrieben werden können (Rousseau et al., 1998; Deutsch, 1958). Deshalb verwundert es auch nicht, dass Vertrauen oft als statische Grösse betrachtet wird. Langley (2007) kritisiert: "We need more process thinking in research (…)" (S. 271). Rousseau et al. (1998) betrachten Vertrauen in ihrer Arbeit als Auslöser, aber ebenso als Resultat von Transaktionen. Dieser mehrdeutigen Rolle von Vertrauen ist dieses Kapitel gewidmet, denn Vertrauen verändert sich über die Zeit, je nach Situation, Information oder Erfahrung des Nutzers (Olson & Olson, 2000): "(…) trust is developed over a process of repeated visits to a site as a user gains experience and believes that his/her expectations are met during the visits" (Urban et al., 2009, S. 182).

Rousseau et al. (1998) unterscheiden drei Phasen von Vertrauen, die Phase der Vertrauensbildung, des Erhalts und des Verlustes, wie in Abbildung 26 dargestellt:

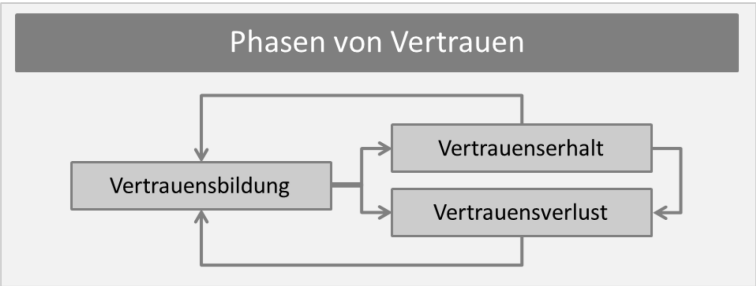


Abbildung 26: Drei Phasen von Vertrauen (eigene Darstellung in Anlehnung an Rousseau et al., 1998)

Vertrauensbildung: In dieser Phase wird Vertrauen gebildet, aufgebaut und reformiert. Das vom Nutzer mitgebrachte Vorschussvertrauen wächst und verändert sich mit der fortschreitenden Dauer der Beziehung. Der Aufbau von Vertrauen be-

ruht demnach auf dem kalkulativen Vertrauen, welches auf einer rationalen Entscheidung, persönlicher Disposition oder auch existierenden Informationen basiert. Kalkuliertes Vertrauen gründet auf glaubwürdiger Information über die Absichten der Vertrauensperson (Rousseau et al., 1998; Jones & George, 1998).

Vertrauenserhalt: In dieser Phase existiert bereits eine vertrauensvolle Beziehung. Mit zunehmender Transaktionsintensität wird das Vertrauen auch relationaler und basiert somit auf den Kenntnissen und Erfahrungen mit dem jeweiligen Transaktionspartner. Dadurch werden Informationen über die Verlässlichkeit der Vertrauensperson gewonnen, und es entsteht ein emotionales Band zwischen den Parteien (Rousseau et al., 1998; Jones & George, 1998). Kim et al. (2004) definieren ein stabiles Vertrauensverhältnis folgendermassen: "Trust is stabilized only when the customer is no longer actively looking for further evidence or reason for placing confidence in the trustworthiness of the Internet store." (S. 393).

Vertrauensverlust: In dieser Phase wird Vertrauen über die Zeit oder durch einen Vertrauensbruch abgebaut. Wird der Nutzer vom Transaktionspartner oder dessen Leistung enttäuscht, kommt es zu einem Vertrauensverlust (Rousseau et al., 1998; Jones & George, 1998). Corritore, Kracher und Wiedenbeck (2003) fügen eine weitere Phase hinzu und schliessen damit den Kreis der Vertrauensbildung: das Wiedererlangen von Vertrauen nach dem Vertrauensverlust.

Diese drei Phasen der Vertrauensbildung können nun dem Online-Entscheidungsfindungsprozess aus Kapitel 2.1.3.2 zugeordnet werden, wie in Abbildung 27 zusammengefasst:

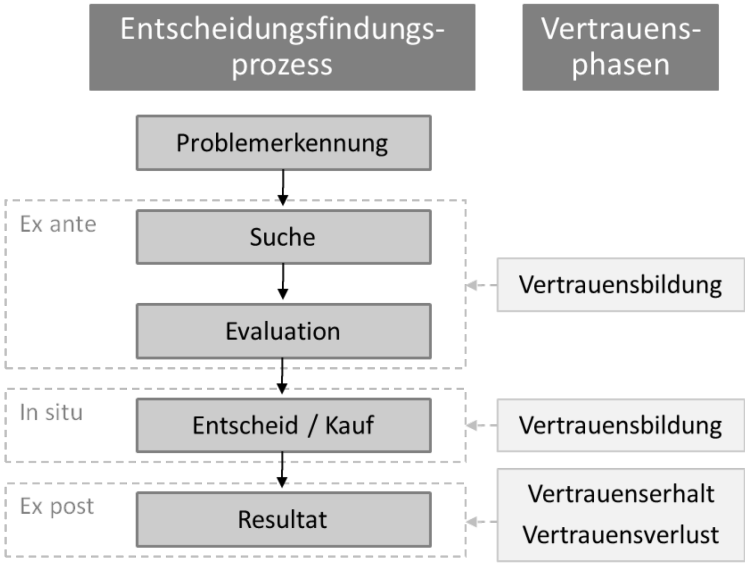


Abbildung 27: Online-Entscheidungsfindungsprozess und die Vertrauensphasen (eigene Darstellung)

Für die erste Phase von Vertrauen, dem Vertrauensaufbau, verwenden Vertrauensforscher auch die Terminologie Initialvertrauen (Initial Trust) für Beziehungen in Situationen, in denen glaubwürdige und aussagekräftige Informationen über die zu vertrauende Partei unbekannt sind (Jones & George, 1998; Koufaris & Hampton-Sosa, 2004; McKnight et al., 1998; McKnight et al., 2002a). In dieser Arbeit wiederspiegeln die Phasen ex ante und in situ das Initialvertrauen, da diese glaubwürdigen und aussagekräftigen Informationen in diesen beiden Phasen des Entscheidungsfindungsprozesses gesammelt und generiert werden und erst in der Ex-post-Phase zur Verfügung stehen, wenn entschieden wird, ob dem Anbieter in Zukunft Vertrauen entgegengebracht werden kann (Vertrauenserhalt) oder nicht (Vertrauensverlust), wie in Abbildung 27 dargestellt. Kim et al. (2004) fassen dies wie folgt zusammen: "(…) trust evolves with the customer's purchase experience with the Internet store from initial trust to stabilized trust" (S. 393). Die Absicht, in Zukunft zu vertrauen, ist Gegenstand des nächsten Kapitels.

2.3.3.2 Die Absicht, in Zukunft zu vertrauen

Die Absicht, einem Anbieter in Zukunft zu vertrauen, basiert auf vergangenen Erfahrungen und dieses Vertrauensverhältnis wiederum entsteht aufgrund wiederholter Transaktionen. Dadurch werden Informationen über die Verlässlichkeit der Vertrauensperson gewonnen, und es entsteht ein emotionales Band zwischen den Par-

teien (Rousseau et al., 1998). Diese Absicht, in Zukunft einem bestimmten Online-Anbieter zu vertrauen, wird mit dem Begriff Vertrauensabsicht bezeichnet.

Vertrauensabsicht (Trusting Intention): Im Kapitel 2.3.1.1 wurde diskutiert, dass Vertrauen die Komplexität von Entscheidungen verringert, indem Unsicherheit und Abhängigkeit in Vertrauen umgewandelt werden (Luhmann, 1979; Riegelsberger & Sasse, 2001). Die Definition der Vertrauensabsicht von McKnight et al. (2002a) geht auf dieses Konzept der Abhängigkeit ein: "Willingness to depend (volitional preparedness to make oneself vulnerable to the trustee) and subjective probability of depending (the perceived likelihood that one will depend on the other) form two distinct subconstructs of trusting intentions." (S. 337). Auch die Autoren Moormann, Deshapande und Zaltman (1993) definieren die Bereitschaft zu vertrauen als „willingness to rely on an exchange partner" (S. 82). Mayer et al. (1995) definieren zukünftiges Vertrauen als „the willingness of a party to be vulnerable to the actions of another party" (S. 712), und zwar in einem Kontext, in dem der Vertrauensnehmer keine Kontrolle über die Situation hat. Die Definitionen der Vertrauensabsicht beinhalten demnach alle die Bereitschaft, Verwundbarkeit zuzulassen oder ein Risiko einzugehen (Euijin & Tadisina, 2007; Schlosser et al., 1993). McAllister (1995) fasst dies zusammen und schreibt, dass Vertrauensabsichten es den Menschen erst ermöglichen, Risiken einzugehen. Mayer et al. (1995) betonen den Unterschied zwischen Vertrauen und der Absicht zu vertrauen: "Trust is the willingness to assume risk; behavioral trust is the assuming of risk." (S. 724).

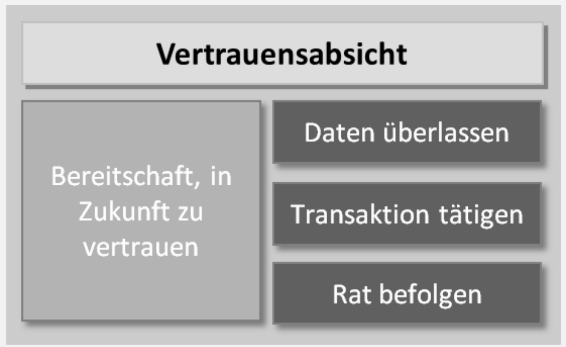


Abbildung 28: Vertrauensabsicht (eigene Darstellung in Anlehnung an McKnight et al., 2002a)

Die Autoren McKnight et al. (2002a) schreiben, dass die subjektive Wahrscheinlichkeit der Nutzer, sich auf den Anbieter zu verlassen, sich in drei Verhaltensweisen äussern kann: dem Anbieter persönliche Informationen zu überlassen, eine Transaktion zu tätigen oder sich gemäss dem Rat des Anbieters zu verhalten (zum Beispiel in finanziellen Angelegenheiten), wie in Abbildung 28 dargestellt. Graber-Kräuter und

Kaluscha (2003) betonen in ihrer Studie: "It is important to keep in mind that intentions do not automatically imply behavior." (S. 804). Die Äusserung einer Absicht alleine genügt nicht, um daraus schliessen zu können, dass der Nutzer das Risiko einer Transaktion auch tatsächlich eingeht (Kräuter & Kaluscha, 2003; McKnight et al., 2002a). Die Absicht ist aber dennoch Grundvoraussetzung für eine mögliche zukünftige Transaktion.

Die Items des Faktors Vertrauensabsicht aus dem Web Trust Model von McKnight et al. (1998; 2002a) wurden für die quantitative Online-Umfrage übernommen (siehe Methodik-Kapitel 3.1.2 und Fragebogen im Anhang 7.4.1).

Gefen und Straub (2003) ebenso wie Lynch, Kent und Srinivasan (2001) haben den Einfluss von Vertrauen auf die Kaufabsicht im Internet untersucht und konnten nachweisen, dass Vertrauen einen signifikanten Einfluss auf die Kaufabsicht hat (ebenso Jarvenpaa & Tractinsky, 1999; Chau et al., 2000; Davis, 1989; Dimitriadis & Kyrezis, 2010). Kim et al. (2004) konnten aufzeigen, dass mit steigender Zufriedenheit der Kunden eine erneute Transaktion wahrscheinlicher wird. Einwiller, Herrmann und Ingenhoff (2005) untersuchten ebenfalls die Einflüsse von Vertrauen auf die Kaufabsicht und konnten nachweisen, dass ein höheres Vertrauen in den Anbieter sich tatsächlich positiv auf eine vertrauensvolle Kaufabsicht auswirkt (s. a. Doney & Cannon, 1997; Bhattacherjee, 2002) und demnach ein Wiederkauf wahrscheinlicher wird (Qureshi, Fang, Ramsey, McCole, Ibbotson & Compeau, 2009). Lynch et al. (2001) vertreten die Meinung, dass die Stärke der Vertrauensneigung sowohl die Kaufbereitschaft als auch die Absicht der Kunden, zur Seite zurückzukehren, bestimmen.

In diesem Kapitel wurde aufgezeigt, dass es unterschiedliche Studien zu den Vertrauensabsichten gibt. Keine dieser Studien unterscheidet jedoch nach der Zielgruppe. Deshalb lautet die dritte und letzte zu untersuchende Forschungsfrage:

Forschungsfrage 3: Unterscheiden sich die Vertrauenstypen in Bezug auf ihre Vertrauensabsichten?

Die Absichten pro Vertrauenstyp werden im Kapitel Methodik (3.2.3) aufgrund des in diesem Kapitel vorgestellten Faktors Vertrauensabsicht analysiert. Im folgenden Kapitel werden die Erkenntnisse aus der theoretischen Betrachtung von Vertrauen zusammengefasst.

2.3.4 Zusammenfassung

Fehlendes Vertrauen wird als Barriere betrachtet, welche Nutzer von Online-Transaktionen abhält (Urban et al., 2009). Vertrauen wird als eine Erwartungshaltung, eine Überzeugung oder ein Gefühl der Betroffenen verstanden und setzt sich aus den wahrgenommenen Komponenten Kompetenz, Ehrlichkeit sowie Wohlwollen zusammen (Belanger et al., 2002; Casalo et al., 2008).

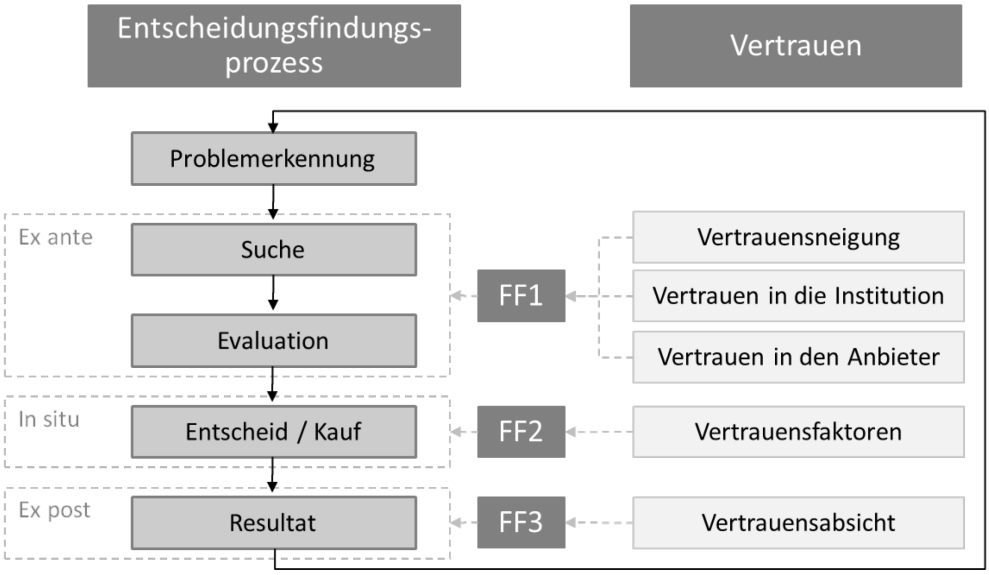


Abbildung 29: Zusammenhang zwischen Vertrauen, dem Entscheidungsfindungsprozess und den Forschungsfragen (eigene Darstellung)

In diesem Kapitel konnte festgestellt werden, dass persönliche Eigenschaften der Nutzer ebenso einen Einfluss auf die Vertrauensbildung im Online-Entscheidungsfindungsprozess entfalten (Vertrauensneigung) wie institutionelle Rahmenbedingungen (Vertrauen in die Institution) oder die Wahrnehmung des Anbieters (Vertrauen in den Anbieter), wie in Abbildung 29 dargestellt. Online-Unternehmen sehen sich mit der Herausforderung konfrontiert, das Vertrauen ihrer Nutzer zu gewinnen und zu pflegen. Individuen bringen aber je nach Typ unterschiedliches Vorschussvertrauen in eine Situation hinein. Die erste Forschungsfrage (FF1) dieser Dissertation befasst sich deshalb mit der Frage, ob unterschiedliche Vertrauenstypen im Internet existieren.

Für Online-Anbieter bestehen verschiedene Möglichkeiten, Vertrauen bei den Nutzern zu fördern. Anhand einer ausführlichen Literaturrecherche wurden zwölf zentrale Faktoren identifiziert, welche einen positiven Einfluss auf die Vertrauensbildung der Nutzer bei Online-Transaktionen haben: Reziprozität, Nutzerkontrolle,

Kommunikation, Marke, Reputation, Siegel und Zertifikate, Nutzerratings, Design, Technik, Sicherheit, Realweltbezug und Kundenservice. Ob diese Vertrauensfaktoren während einer Transaktion im Internet von Personengruppe zu Personengruppe unterschiedlich wahrgenommen werden, ist Gegenstand der zweiten Forschungsfrage (FF2) (Abbildung 29).

Vertrauen ist einerseits Auslöser, aber ebenso Resultat von Transaktionen. Es können drei Phasen der Vertrauensbildung unterschieden werden: die Phase der Vertrauensbildung, des Erhalts und des Verlustes (Rousseau et al., 1998). Befindet sich der Nutzer in der Such- und Evaluationsphase, kann, ebenso wie bei der Transaktion selbst, Vertrauen aufgebaut werden. Nach Vollendung der Transaktion wird bei Erfüllung Vertrauen erhalten und bei Nichterfüllung Vertrauen zerstört. Die Absicht, einem Anbieter in Zukunft zu vertrauen, basiert auf vergangenen Erfahrungen und dieses Vertrauensverhältnis wiederum entsteht aufgrund wiederholter Transaktionen. Die dritte Forschungsfrage (FF3) untersucht die Beziehung zwischen der Vertrauensabsicht und den Vertrauenstypen (Abbildung 29).

Nachdem nun die theoretischen Grundlagen erläutert wurden, wird im folgenden Kapitel das forschungsmethodische Vorgehen der Dissertation zur Beantwortung der drei Forschungsfragen vorgestellt.

3 Forschungsmethodisches Vorgehen

Dieses Kapitel wurde in zwei Bereiche aufgeteilt, in die forschungsmethodischen Vorarbeiten sowie in die Hauptuntersuchung (siehe Abbildung 30). Das Kapitel 3.1 „Forschungsmethodische Vorarbeiten“ geht auf die für die Beantwortung der Forschungsfragen nötigen Vorarbeiten im qualitativen und quantitativen Bereich ein. Im Kapitel 3.2 „Hauptuntersuchung“ werden die definierten Forschungsfragen anhand der Auswertungsmethoden Clusteranalyse, Diskriminanzanalyse sowie Mittelwertvergleich im Detail besprochen.

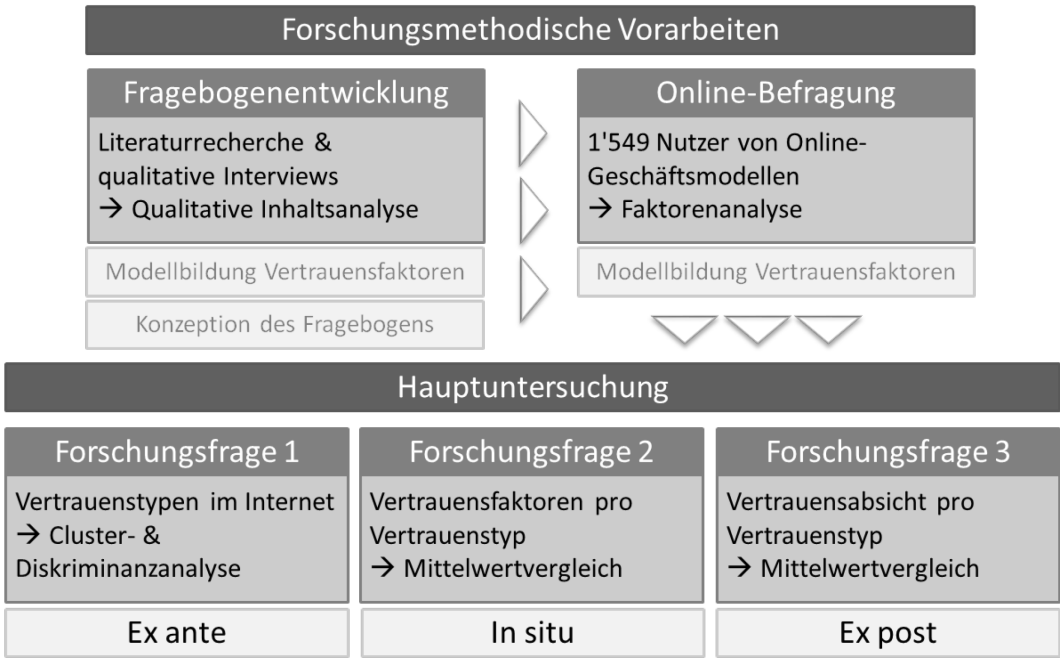


Abbildung 30: Forschungsmethodisches Vorgehen (eigene Darstellung)

3.1 Forschungsmethodische Vorarbeiten

In diesem Kapitel werden die forschungsmethodischen Vorarbeiten diskutiert, welche für die Durchführung der Hauptuntersuchung nötig sind. Im ersten Kapitel 3.1.1 werden das Auswahlverfahren für die qualitativen Interviews mit Anbietern und Nutzern von Online-Geschäftsmodellen erläutert sowie die Durchführung der Interviews und deren Auswertung beschrieben. In dieser qualitativen Phase werden jene Elemente herausgearbeitet, die aus Sicht der Anbieter bei Nutzern und aus Sicht der Nutzer Vertrauen im Umgang mit Daten im Rahmen digitaler Transaktionen erzeugen. Die Vertrauensfaktoren wurden im Rahmen der Literaturrecherche identifiziert und anhand der Interviews verdichtet und ergänzt, bevor sie in einer breit angelegten Online-Umfrage von den Nutzern gewichtet und priorisiert werden, um darauf basierend Vertrauenstypen zu identifizieren. Im zweiten Kapitel 3.1.2 werden die Konzeption des Fragebogens sowie die Durchführung der quantitativen Befragung vorgestellt, während im dritten Kapitel 3.1.3 spezifisch auf den Untersuchungskontext eingegangen wird. In Kapitel 3.1.4 werden durch die Auswertung der Vertrauensfaktoren und des Vertrauensmasses die ersten quantitativen Analysen vorgenommen. Anhand von Faktorenanalysen werden relevante Vertrauensfaktoren aus Sicht der Nutzer sowie das Vertrauensmass identifiziert, welche in der Hauptuntersuchung aufgegriffen werden. Im Kapitel 3.1.5 werden die forschungsmethodischen Vorarbeiten zusammengefasst.

3.1.1 Qualitative Befragung von Anbietern und Nutzern von Online-Geschäftsmodellen

Im Theorie-Kapitel 2.3.2.2 wurde bereits ein Bündel von zwölf relevanten Vertrauensfaktoren besprochen. Die qualitativen Befragungen dienen nun dazu, diese aus der Literatur aufgearbeiteten Vertrauensfaktoren zu validieren, zu verdichten, zu ergänzen oder zu differenzieren. Um vertiefte Einblicke in die Wahrnehmung von Vertrauen durch die betroffenen Anbieter sowie der Nutzer erlangen zu können, wird für die Erhebung der Daten der interpretative Forschungsansatz (Denzin, 1983) angewendet und für die Auswertung der Ansatz der qualitativen Inhaltsanalyse verfolgt (Gläser & Laudel, 2006; Mayring, 1991). Diese beiden Forschungsansätze werden im Folgenden näher erläutert.

Interviews mit Anbietern von Online-Geschäftsmodellen: Im Zeitraum von Juni bis Oktober 2009 wurden 23 Vertreter von 21 Online-Geschäftsmodellen befragt, welche im deutschen Markt tätig sind (Abbildung 31). Die Auswahl der Anbieter von Online-Geschäftsmodellen basiert auf der Systematik von Timmers (1998), welche in diesem Zusammenhang als eines der bekanntesten Konzepte gilt (Afuah & Tucci, 2001; Lambert, 2006). Unterschieden wurden die folgenden vier Online-Geschäftsmodelle: Online-Shopping, Online-Banking, soziale Netzwerke und Online-Information. Die Operationalisierung des Konzeptes von Timmers (1998) wurde im Kapitel 2.1.1.3 beschrieben. Die detaillierte Zusammenstellung der befragten Anbieter befindet sich im Anhang 7.2.2. Gemäss dem Konzept des theoretischen Samplings folgten Zusammensetzung und Umfang der Stichprobe der Zielvorgabe der theoretischen Sättigung (Glaser & Strauss, 1967). So wurde die Stichprobe schrittweise um Vertreter etablierter und junger Unternehmen erweitert – darunter bekannte Marken wie Google, eBay und Xing, aber auch kleinere Anbieter und Start-ups wie Experteer, Mitfahrzentrale oder Wunderloop.

Abbildung 31: Interviewte Anbieter von Online-Geschäftsmodellen (eigene Darstellung)

Da das spezifische Fachwissen der Experten und nicht die Gesamtperson Gegenstand der Analyse ist, wurde die Datenerhebung in Form von Experteninterviews durchgeführt (Bähring, Hauff, Sossdorf & Thommes, 2008).

Gewählt wurde das problemzentrierte Interview[26] anhand eines halbstandardisierten Fragebogens (Witzel, 1982). Die Teilnehmer wurden jeweils in circa halbstündigen Telefoninterviews nach dem Stellenwert des Nutzervertrauens in der Unternehmenspraxis befragt und gebeten, mögliche und sinnvolle Massnahmen zur Steigerung des Vertrauens zu beschreiben. Der Interviewleitfaden der Anbieter (siehe Anhang 7.2.1) baute auf den aus der Literatur generierten Erkenntnissen auf und wurde in drei Hauptkomponenten unterteilt: Das erste Modul diente dem Einstieg, dem gegenseitigen Kennenlernen und der Einführung in das Thema Trust Management im Internet und widmete sich der Bedeutung des Kundenvertrauens im Allgemeinen. Das zweite Modul beschäftigte sich mit den vertrauensrelevanten Faktoren aus Sicht der Anbieter. Der letzte Block befasste sich mit Vertrauen in der Unternehmenskommunikation und in der Öffentlichkeitsarbeit.

Interviews mit Nutzern von Online-Geschäftsmodellen: Im Zeitraum von Februar bis April 2010 wurden 43 deutsche Internetnutzer in persönlichen oder telefonischen Gesprächen in der Länge von 20 bis 30 Minuten zum Thema Vertrauen im Internet befragt (Abbildung 32). Die detaillierte Zusammenstellung der interviewten Nutzer befindet sich im Anhang 7.3.2. Der Interviewleitfaden der Nutzer (siehe Anhang 7.3.1) wurde ebenfalls in drei Hauptkomponenten unterteilt. Wie bei den Anbieterinterviews diente das erste Modul dem Einstieg und dem gegenseitigen Kennenlernen. Im zweiten Modul wurden die Nutzer über ihr Internetnutzungsverhalten befragt, um danach im dritten Modul auf die einzelnen vertrauensfördernden Faktoren einzugehen.

[26] Witzel (1982) beschreibt problemzentrierte Interviews als eine Interview-Variante, „die eine sehr lockere Bindung an einen knappen, der thematischen Orientierung dienenden Leitfaden mit dem Versuch verbindet, den Befragten sehr weitgehende Artikulationschancen einzuräumen und zu freien Erzählungen anzuregen“ (zit. in Hopf, 1991, S. 178). In ein problemzentriertes Interview können, je nach Gesprächsverlauf, Konfrontationsfragen oder theoriegeleitete Fragen eingebracht werden. Voraussetzung dafür ist, dass der Interviewpartner über einen komplexen Wissenshintergrund zum Thema der Untersuchung verfügt (Flick, 2002). Gestützt durch einen Leitfaden kann der Interviewer im Verlauf der Befragung entscheiden, wann und in welcher Reihenfolge er welche Fragen stellt, um einen natürlichen Gesprächsverlauf zu fördern. Einerseits können Fragen, die schon beantwortet wurden, übersprungen werden oder der Interviewer kann zu Fragen zurückkehren, die übergangen wurden. Andererseits kann bei einer Abschweifung vom Thema auf den Fragebogen zurückgegriffen werden (Flick, 2002.; Gläser & Laudel, 2006).

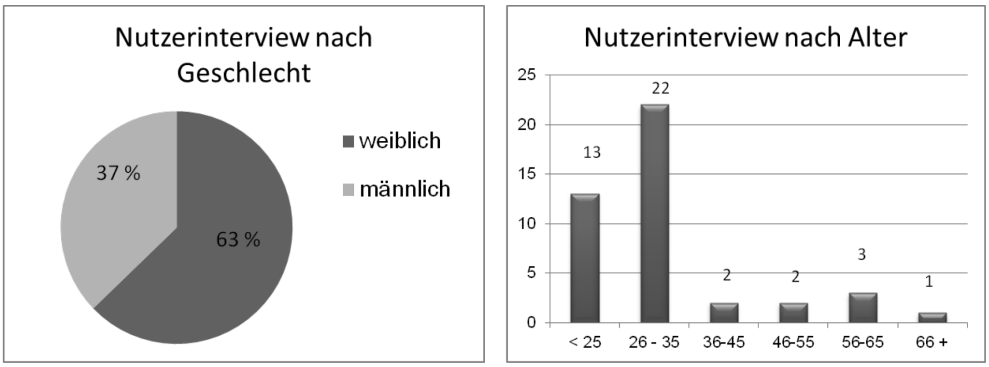


Abbildung 32: Interviewte Nutzer von Online-Geschäftsmodellen (eigene Darstellung)

Datenauswertung anhand der qualitativen Inhaltsanalyse: Alle Interviews wurden aufgezeichnet und im Anschluss transkribiert. Dies geschah, um die Gefahr der Unübersichtlichkeit zu verringern und um zu verhindern, dass die Sinnhaftigkeit einzelner Aussagen ausserhalb des Gesprächskontextes verloren geht (Gläser & Laudel, 2006). Die Transkripte wurden anschliessend auf Kommentare, Sätze und Satzfragmente analysiert, die mit der Wahrnehmung und den Meinungen zu den Treibern der Vertrauenswürdigkeit eines Unternehmens, den Wahrnehmungen der Nutzer von vertrauensbildenden Faktoren sowie dem Engagement des Geschäftsmodell-Anbieters im Vertrauensmanagement in Beziehung gesetzt werden können. Dadurch wurde es möglich, die Faktoren aus der Theorie mit den Beschreibungen durch die Interviewpartner zu vergleichen. In dieser Phase werden alle relevanten Satzfragmente in Kategorien eingeteilt (Mayring, 1991). Ausserdem wird auf Schlüsselwörter, auffallende Häufigkeiten, Widersprüche und pointierte Aussagen geachtet. Die Beschriftung dieser Kategorien wird an den Rand der Abschrift des Experteninterviews geschrieben. Ziel ist es, das Gemeinsame aus den Interviews herauszuarbeiten und Deutungsmuster herauszukristallisieren (Meuser & Nagel, 1991). Bei den Überschriften der verschiedenen Kategorien werden Terminologien der Interviewten verwendet (Meuser & Nagel, 1991). Die einzelnen Kategorien werden danach den zwölf in der Theorie identifizieren Vertrauensfaktoren zugeordnet, damit so die Häufigkeiten des Auftretens von Kategorien im Text ermittelt werden kann. Je häufiger einzelne Kategorien vorkommen, desto bedeutender sind die Sachverhalte. Durch diese Analyse verschafft man sich eine Informationsbasis, die nur noch jene Informationen enthält, welche für die Beantwortung der Untersuchungsfragen tatsächlich relevant sind (Gläser & Laudel, 2006).

Gütekriterien der qualitativen Forschung: Die Qualität der Forschungsergebnisse wird anhand der klassischen Gütekriterien von Mayring (2002) sichergestellt: (1) Ver-

fahrensdokumentation: Der Forschungsprozess muss für Dritte nachvollziehbar sein, was durch die ausführliche Dokumentation des Forschungsprozesses gewährleistet wird. (2) Regelgeleitetheit: Um dem Gegenstand der Forschung näherzukommen, ist ein systematisches Vorgehen anhand von Analyseschritten zu wählen. Dies wird anhand der beiden theoriegenerierten Interviewleitfäden sichergestellt. (3) Kommunikative Validierung: Auf die kommunikative Validierung durch die Erforschten wird verzichtet, da der Grossteil der Interviews anonym durchgeführt wurde. Als Massnahme zur Qualitätssicherung wird Transparenz durch die Dokumentation und Reflexion des Forschungsprozesses hergestellt (Bähring et al., 2008). (4) Triangulation: Durch die Verbindung der theoretischen Erkenntnisse sowie der Erkenntnisse aus Anbietersicht und aus Nutzersicht wird die Qualität der Ergebnisse erhöht.

Ergebnisse der qualitativen Forschung: Die Analyse der Ansichten und Meinungen der Interviewpartner konnte die aus der Theorie abgeleiteten zwölf Vertrauensfaktoren auf neun relevante Faktoren verdichten (Abbildung 24 im Vergleich zu Abbildung 33).

Abbildung 33: Relevante Vertrauensfaktoren (Hoffmann, Meckel & von Kaenel, 2010b)

Die neun relevanten Vertrauensfaktoren (Abbildung 33), identifiziert aus der Theorie und validiert im praktischen Kontext, werden im Folgenden kurz beschrieben: (1) Die **Reziprozität**, das Verhältnis von Risiko und Nutzen aus Sicht des Nutzers. Online-Unternehmen müssen sich bemühen, eine Bereitstellung der persönlichen Daten durch einen angemessenen Nutzengewinn zu kompensieren (Das & Teng, 1998; Lanier & Saini, 2008; Chellappa & Sin, 2005; Ashworth & Free, 2006). (2) Die **Nutzerkontrolle**, das heisst, der Nutzer kann selbst bestimmen, wer welche Daten von ihm einsehen und verwenden kann (Culnan & Armstrong, 1999; Milne & Boza, 1999; Phelps et al., 2001). (3) Die **proaktive Kommunikation** des Unternehmens in Bezug auf die Privatsphäre und der Sicherheit der Daten (Chadwick, 2001; Geyskens et al., 1998; Lewicki & Bunker, 1995; Morgan & Hunt, 1994; Speier et al., 1998). (4) Die **Marke** und somit Sympathie, Image sowie die Reputation des Unternehmens (Cor-

bitt et al., 2003; Ha & Perks, 2005; Jevons & Gabbott, 2000; Walczuch & Lundgren, 2004; Eastlick et al., 2006; Milne & Boza, 1999). (5) **Empfehlungen** durch Drittpersonen können zum Beispiel Bewertungen durch die Stiftung Warentest oder andere qualifizierte Qualitätskennzeichen, aber auch Nutzerratings sein (Corbitt et al., 2003; Kovar, Burke & Kovar, 2000; Luo & Cook, 2007–2008; Shneiderman, 2000). (6) Das **Design** der Benutzeroberfläche, die Darstellung und die wahrgenommene Seriosität des Unternehmens (Egger, 2000; Chau et al., 2000; Shneiderman, 2000). Darüber hinaus konnte die Studie zeigen, dass (7) die **Technik**, bzw. die Zuverlässigkeit der technischen Infrastruktur (Bhatnagar et al., 2000; Lee & Turban, 2001) einen weiteren bedeutenden Vertrauenstreiber darstellt. Reine Online-Anbieter können Vertrauen auch dadurch erzeugen, dass sie einen (8) **Realweltbezug** herstellen, etwa durch die umfassende Angabe von Kontaktmöglichkeiten oder die Abbildung ihrer Mitarbeiter und Räumlichkeiten (Jarvenpaa & Tractinsky, 1999). Nicht zuletzt fördert auch das Bereitstellen eines (9) hilfreichen und freundlichen **Kundenservices** das Nutzervertrauen (Brinkmann & Seifert, 2001; Lee & Turban, 2001; McAllister, 1995; Olivero & Lunt, 2004). Die vertiefte Diskussion der einzelnen Faktoren können in Theorie-Kapitel 2.3.2.2 nachgelesen werden.[27]

Im Vergleich zu den Ergebnissen aus dem Theoriekapitel (2.3.2.2) fällt auf, dass die Interviewpartner die Faktoren Marke und Reputation als einen einzigen Faktor „Marke" wahrnehmen: *„Und wo empfindet der Verbraucher Vertrauen? Das ist in der Tat bei bekannten Portalen, so wie bei uns, wo auch eine Marke hinter steckt, ganz klar, also mit (…) verbindet man was, wo eben auch der Ruf gut ist (…)"* (A4, 05.03.2009)[28] oder *„(…) es gibt einfach bestimmte Dienste (…) denen vertraue ich, weil es vielleicht auch einfach etablierte Dienste sind, die eine Nutzerbasis von Hunderttausend, Millionen Leuten haben, wo ich davon ausgehe, dass die sich das gar nicht leisten können, dann fehlerhaft mit meinen Daten umzugehen (…)"* (N3, 03.03.2010). Ebenfalls verstehen die Interviewpartner die Faktoren Gütesiegel, Zertifikate und Nutzerratings als einen Faktor – er wird in dieser Arbeit unter „Empfehlungen" zusammengefasst: *„Bei uns aber mindestens genauso wichtig [wie Gütesiegel] ist die Empfehlung über die Nutzer selbst. Ich hatte einen Bekannten, einen Freund, der war schon da, oder meine Tochter oder mein Sohn hat gesagt, ich soll*

[27] Die Ergebnisse der qualitativen Interviews wurden auf der Konferenz der International Communication Association (ICA) in Singapur vorgestellt (Hoffmann, Meckel & von Kaenel, 2010b).

[28] A = Anbieter und N = Nutzer

doch mal … das ist relevant" (A12, 12.03.2009) oder *„Und eigentlich ist es am besten, wenn man so was hört von Bekannten, von Freunden, die sagen, das ist am besten oder wenn gerade so was wie Stiftung Warentest es mal richtig durchcheckt*" (N37, 27.04.10). Weiter differenzieren Nutzer und Anbieter nicht zwischen den Faktoren Technik und der Sicherheitsinfrastruktur im Netz, diese beiden Faktoren werden unter dem Faktor „Technik" subsumiert: *„Also, die Sicherheit, also das technische Know-how dahinter, das ist glaube ich ein grosser Vertrauensfaktor*" (A7, 04.03.2009) oder *„(…) bei Kreditkarten (…) hat man immer ein bisschen ein komisches Gefühl, aber ich glaube mittlerweile ist die Technik so weit, dass ich dem jetzt vertraue*" (N13, 09.03.2010).

Aufgrund der Interpretation der Faktoren aus Sicht der Anbieter und Nutzer wird in dieser Arbeit nun nicht mehr von den zwölf, sondern von den neun Faktoren ausgegangen. Die einzelnen Items zu den jeweiligen Faktoren wurden aus der Literaturrecherche im Theoriekapitel abgeleitet (siehe Kapitel 2.3.2.2) und aufgrund der qualitativen Interviews kontinuierlich angepasst und validiert. Die finale Liste der Items befindet sich im Anhang 7.4.3.

Im folgenden Kapitel wird die Konzeption des Fragebogens und die quantitative Datenerhebung für die Online-Umfrage vorgestellt.

3.1.2 Fragebogenkonzeption und quantitative Datenerhebung

Für die Beantwortung der in Kapitel 1.2.1 vorgestellten Forschungsfragen wurde die Datenerhebung anhand einer Online-Befragung gewählt. Ein Vorteil der Online-Befragung ist, dass die Datenerhebung sowie die Datenauswertung kurze Antwortzeiten ermöglichen und relativ geringe Kosten verursachen (Harris, 1997). Durch die Anonymität des Mediums Internet ist es möglich, sensiblere Fragen als in einer persönlichen Befragung zu stellen (Batinic, 2001; Hewson, Yule, Laurent & Vogel, 2003; Pealer, Weiler, Pigg, Miller & Dorman, 2001) und der Einfluss des Interviewenden auf die Probanden entfällt (Hewson et al., 2003). Ein Nachteil von Online-Befragungen ist, dass nur diejenige Bevölkerungsschicht befragt werden kann, die das Internet bereits nutzt, und dass durch das Auslassen der Nicht-Nutzer die Bevölkerungsrepräsentativität verzerrt wird. Des Weiteren ist eine Online-Umfrage eine Erhebung zu einem gewissen Zeitpunkt in einem spezifischen Transaktionskontext. Möglich ist auch, dass Sicherheits- und Datenschutzbedenken die Probanden von der Teilnahme abhalten können, oder aber, dass einzelne Personen sinnlose oder falsche Angaben machen und somit die Ergebnisse der Befragung verfälschen (Ba-

tinic, 2001). Nach Batinic (2001) kann aber davon ausgegangen werden, dass Online-Befragungen mit der klassischen Offline-Befragung in puncto Validität gleichgesetzt werden können.

Die Konzeption des Fragebogens: Für die Befragung wird ein standardisierter Fragebogen entwickelt, welcher die zentrale Basis zur Beantwortung der definierten Forschungsfragen bildet. Der Fragebogen für die Online-Befragung basiert auf den Ergebnissen der qualitativen Interviews sowie auf den aus der Literatur generierten Erkenntnissen. Der Fragebogen wird mithilfe der Plattform Unipark programmiert. Ein Printscreen des Fragebogens befindet sich im Anhang 7.4.1 dieser Arbeit. Wie aus Abbildung 34 hervorgeht, ist die Befragung in fünf Hauptkomponenten gegliedert.

Abbildung 34: Konzeption des Fragebogens (eigene Darstellung)

Der Fragebogen beginnt mit einer Begrüssungsseite, auf der das Forschungsvorhaben vorgestellt, die Universität St. Gallen als Absender identifiziert und die durchschnittliche Bearbeitungsdauer angegeben wird. Ausserdem wird den Befragten Anonymität und Vertraulichkeit zugesichert. Danach werden statistische Angaben zur Person abgefragt: Geschlecht, Alter, höchster Bildungsabschluss, Erwerbstätigkeit und Branche. Im zweiten Modul werden Fragen zur Internetnutzung (täglich bis weniger als einmal im Monat), der Nutzungsdauer (Anzahl Jahre) und der Art der Nutzung (beruflich oder privat) erhoben. Auch wird gefragt, welche Online-Dienste von den Teilnehmern wie oft genutzt werden. Im dritten Modul werden das Institutionsvertrauen, die Vertrauensneigung, welche aus dem Web Trust Model von McKnight et al. (1998; 2002a) abgeleitet wurden (siehe Kapitel 2.3.1.3), sowie die persönlichen Internetkompetenzen im Allgemeinen abgefragt. Das vierte Modul beginnt damit, dass der Befragte den spezifischen Online-Anbieter benennen muss, bei dem er sich als Letztes registriert hat. Zur Auswahl stehen dem Befragten die vier Online-Geschäftsmodelle, welche nach Timmers (1998) operationalisiert wurden (siehe Kapi-

tel 2.1.1.3): Online-Shopping, Online-Banking, soziale Netzwerke und Online-Information. Danach werden Fragen zur Einschätzung des jeweiligen Anbieters und über die potenzielle zukünftige Nutzung des Anbieters gestellt (Items übernommen von McKnight et al., 1998; 2002a; Casalo et al., 2008). Das letzte Modul bezieht sich immer auf den ausgewählten Anbieter aus Modul vier und ist in einen spezifischen Transaktionskontext eingebettet. Die Teilnehmer werden gebeten, Eigenschaften des Anbieters zu beurteilen, welche einen möglichen Einfluss auf ihren Entscheid zur Registrierung hatten. Diese Eigenschaften werden aufgrund der neun Faktoren in Form von 50 Items abgefragt (Anhang 7.4.1), welche im Theorieteil (Kapitel 2.3.2.2) und durch die qualitativen Interviews (Kapitel 3.1.1) erarbeitet wurden. Zum Abschluss wird detailliert erhoben, welche persönlichen Daten bei der Registrierung angegeben werden mussten. Danach wird den Teilnehmern gedankt und die Befragung schliesst mit einer Verabschiedung.

Alle Fragen können vom Befragten übersprungen werden, da keine der Fragen als Pflichtfrage definiert wurde. Dadurch soll verhindert werden, dass Teilnehmer die Umfrage aufgrund zu sensibler Fragen abbrechen. Die Bewertung der Aussagen erfolgt anhand einer fünfstufigen Likert-Skala mit den Endpunkten „trifft zu“ / „trifft nicht zu“ sowie „stark beachtet“ / „nicht beachtet“. Da bei den einzelnen Vertrauensfaktoren mehr als 50 Items abgefragt werden, besteht die Möglichkeit, dass der Befragte ermüdet und, besonders gegen Ende des Fragebogens, die Aufmerksamkeit nachlässt. Dieser „Fatigue Effect“ führt dazu, dass einzelne Fragen schematisch beantwortet werden (Brace, 2004). Dem wird mittels Randomisierung entgegengewirkt. Die Items rotieren automatisch, was einer Verzerrung der Ergebnisse durch den „Fatigue Effect“ entgegenwirkt (Brace, 2004). Die Bearbeitung des gesamten Online-Fragebogens dauert ca. 15 Minuten. Bei längeren Bearbeitungszeiten besteht, insbesondere bei Online-Fragebögen, die Gefahr, dass der Befragte den Fragebogen abbricht (Crawford, Couper & Lamias, 2001; Harris, 1997). Eine Statusanzeige zeigt dem Teilnehmer in Prozent an, wie viel er bereits ausgefüllt hat.

Pretest: Um einen fehlerfreien Ablauf der Befragung zu gewährleisten, wird vor dem Versand des Fragebogens ein Pretest durchgeführt. In dieser Pilotphase wird der Fragebogen auf die Länge (Zeitdauer), die Gestaltung, die Reihenfolge sowie auf seine Verständlichkeit hin untersucht (Hunt, Sparkman & Wilcox, 1982). Vier Experten der Medien- und Kommunikationsforschung begutachten mittels Test-Link den Fragebogen mit besonderem Fokus auf die Validität und Reliabilität der Items. Anschliessend nehmen 34 Personen an der Umfrage teil und hinterlassen, wenn nötig,

Kommentare zu den Fragen. Daraufhin werden geringfügige Änderungen wie Fragenreihenfolge oder Umformulierungen vorgenommen.

Durchführung der quantitativen Online-Befragung: Der Fragebogen wird zwischen Dezember 2010 und Januar 2011 über das Online-Panel der Firma Panelbiz an 11'846 Internetnutzer als Link per E-Mail verteilt. Panelbiz ermöglicht den Zugang zu einem für Deutschland bevölkerungsrepräsentativen Panel. Die Stichprobe wird nach Geschlecht und Alter (Destatis, 2010a; 2010b) quotiert. Gemäss Kotler und Bliemel (2001) ist die grösste Herausforderung einer Online-Umfrage die Ansprache und die Motivation der potenziellen Teilnehmer. Als Incentive dient daher eine Vergütung von 1.95 € pro ausgefülltem Fragebogen, welche vom Marktforschungsinstitut ausbezahlt wird. Diese Aufwandsentschädigung wird als Mittel zur Erhöhung der Teilnehmerbereitschaft sowie als Motivation, den Fragebogen nicht frühzeitig abzubrechen, eingesetzt (Theobald, 2001; Crawford et al., 2001).

1'549 Personen nahmen an der Umfrage teil, dies ergibt eine Rücklaufquote von 13.1 %. Die Zusammensetzung der Stichprobe befindet sich im Anhang 7.4.2. Die Stichprobe von 1'549 weist eine Übervertretung regelmässiger Internetnutzer im Vergleich zur Grundgesamtheit Deutschlands auf: Fast 92 % der Befragten nutzen das Internet täglich, während 2009 in Deutschland nur 67 % das Internet zumindest gelegentlich benutzen (van Eimeren & Frees, 2009). Diese Verzerrung kann durch die Rekrutierungsmethode erklärt werden, da die Probanden per E-Mail zur Umfrage eingeladen wurden. 25 % der männlichen und 40 % der weiblichen Bevölkerung Deutschlands nutzen das Internet nicht und wurden somit von vornherein aufgrund der Befragungsform der quantitativen Umfrage ausgeschlossen (van Eimeren & Frees, 2009).

3.1.3 Untersuchungskontext

Eine Online-Umfrage ist immer eine Erhebung zu einem gewissen Zeitpunkt in einem spezifischen Kontext. Die Probanden wurden im ersten Block nach den demografischen Angaben, zur Internetnutzung und zur Vertrauensneigung sowie zu den Internetkompetenzen befragt. Der zweite Block mit den Fragen zum Geschäftsmodell, dem Vertrauen in den Anbieter, den Vertrauensabsichten sowie den Items der Vertrauensfaktoren wurde in einem spezifischen Transaktionskontext abgefragt: „Denken Sie an den letzten Online-Anbieter, bei dem Sie sich als Nutzer registriert haben, wobei die Anmeldung die Eingabe einiger persönlicher Daten erforderte (z. B.

für das Anlegen eines persönlichen Nutzer-Profils). Um welche Art von Online-Angebot handelte es sich dabei? Bitte wählen Sie aus der folgende Liste: (…)“ (vergleiche Anhang 7.4.1). Die Fragen in diesem Block beziehen sich alle auf den jeweiligen Anbieter, bei welchem sich die Probanden als Letztes angemeldet haben. Im eigentlichen Sinne steht deshalb bei diesem Frageblock kein isolierter Vertrauenstyp sondern ein Transaktionsvertrauenstyp oder Interaktionsvertrauenstyp im Zentrum. Die drei definierten Forschungsfragen tragen dieser Abhängigkeit der Vertrauenstypen vom jeweiligen Transaktionskontext bereits Rechnung, indem sie sich jeweils auf die drei Phasen ex ante, in situ und ex post des Entscheidungsfindungsprozesses (Kapitel 2.1.3) beziehen.

Die erste Forschungsfrage „Existieren bei Internetnutzern unterschiedliche Vertrauenstypen?“ wird anhand einer Clusteranalyse mit den Faktoren Vertrauensneigung (ex ante), Vertrauen in die Institution (ex ante) und Vertrauen in den Anbieter (ex ante) gerechnet. Diese drei Faktoren bringt der Nutzer durch sein Grund- oder Vorschussvertrauen in den Untersuchungskontext mit ein (Rotter, 1967). Wie in Abbildung 12 auf Seite 45 dargestellt, ist der Entscheidungsfindungsprozess des Nutzers ein Kreislauf voller gegenseitiger Wechselbeziehungen: Die Assoziationen, die mit einem Anbieter verbunden sind, sowie das Vertrauen oder Misstrauen, welches gegenüber Drittparteien aufgebracht wird, verändern sich durch eigene Erfahrungen, Erfahrungsberichte von Drittpersonen oder durch weitere Informationen und passen sich stetig an (Darley et al., 2010).

Die zweite Forschungsfrage „Sind während einer Transaktion im Internet für die unterschiedlichen Vertrauenstypen dieselben Vertrauensfaktoren relevant?“ bezieht sich nun explizit auf den jeweiligen Transaktionskontext (in situ). Auf was achtet welcher Vertrauenstyp, während er eine Transaktion durchführt? Die 50 Items, aus welchen die Faktoren gebildet werden (Kapitel 3.1.4), wurden in der Umfrage mit dem Hinweis auf den letzten Online-Anbieter, bei dem sich der Nutzer registriert hat, abgefragt: „Wie stark haben Sie auf folgende Eigenschaften geachtet, als Sie sich beim ausgewählten Anbieter angemeldet haben? Bitte beziehen Sie sich dabei auf den oben genannten Anbieter.“ (Anhang 7.4.1). Alle Faktoren wurden demnach in Bezug auf die vorgenommene Registrierung in einem spezifischen Transaktionskontext vorgenommen.

Die dritte Forschungsfrage befasst sich mit dem mutmasslichen Verhalten, nachdem die Transaktion abgeschlossen ist: „Unterscheiden sich die Vertrauenstypen in Bezug auf ihre Vertrauensabsichten?“ Für die Beantwortung dieser Forschungsfrage

wurde der Faktor Vertrauensabsicht in der Analyse verwendet. Da es sich eindeutig um Fragen über die Zukunft handelt, wurde dieser Frageblock im Online-Fragebogen eingeleitet mit: „Bitte beurteilen Sie die folgenden Aussagen: (…)“. Damit stets klar ist, auf wen sich die jeweiligen Fragen beziehen, wurde bei den einzelnen Items bei jeder Frage auf den jeweiligen Anbieter verwiesen.

3.1.4 Auswertung der Vertrauensfaktoren und des Vertrauensmasses

Bevor in die Hauptuntersuchung eingestiegen werden kann, werden die 50 im Fragebogen abgefragten Items auf Faktoren reduziert, um unterschiedliche Vertrauenstypen anhand deren Bewertung differenzieren zu können. Diese Dimensionsreduktion erfolgt mithilfe einer explorativen Faktorenanalyse, das heisst, vor der Durchführung der Analyse liegen keine Hypothesen über das zu erwartende Ergebnis vor (Backhaus, Erichson, Plinke & Weiber, 2011). Ziel der Faktorenanalyse ist die Datenreduktion, indem eine grosse Anzahl manifester Variablen (auch Items genannt) in wenige Faktoren (auch latente Variablen genannt) zusammengefast werden (Backhaus et al., 2011; Arminger, 1979; Überla, 1977). Dabei zeigen die jeweiligen Faktorladungen an, wie stark eine Variable mit dem Faktor verbunden ist (Geider, Rogge & Schaaf, 1982). Korrelieren einzelne Faktoren untereinander (Korrelation > 0.5), kann davon ausgegangen werden, dass diese das Gleiche darstellen, und diese Variablen können zu einem Faktor zusammengefasst werden. Die resultierenden Faktoren sollten untereinander unkorreliert sein.

Wie in Abbildung 35 dargestellt, wird die explorative Faktorenanalyse in sechs Schritten durchgeführt. Um die Faktorenextraktion durchführen zu können, müssen die Daten zunächst bereinigt, die Variablen ausgewählt und eine Korrelationsmatrix erstellt werden. Danach werden die Kommunalitäten (Extraktionswerte) und die Zahl der Faktoren bestimmt, damit die Faktoren interpretiert werden können.[29]

[29] Backhaus et al. (2011) bestimmt zudem noch die einzelnen Faktorenwerte, diese werden jedoch für die weiteren Analysen nicht benötigt und deshalb ausgelassen.

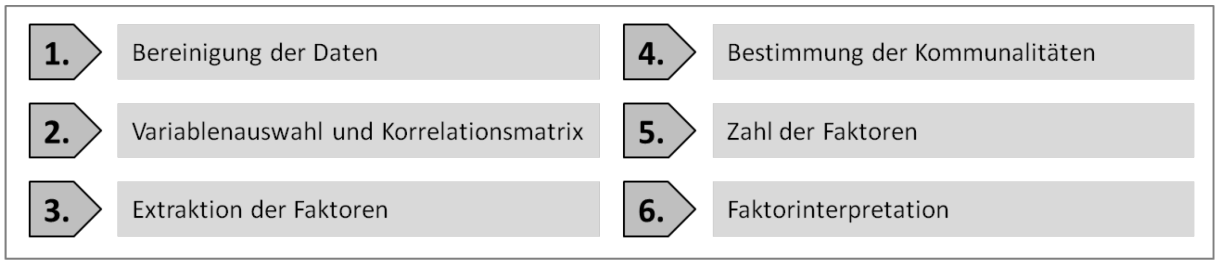


Abbildung 35: Ablaufschritte der Faktorenanalyse (eigene Darstellung in Anlehnung an Backhaus et al., 2011)

Gemäss Backhaus et al. (2011) ist die Güte der Ergebnisse der Faktorenanalyse von der Qualität der Ausgangsdaten abhängig. Damit eine Faktorenanalyse vorgenommen werden kann, empfehlen die Autoren, die Variablen an eine Normalverteilung (NV) anzupassen. Die erhobenen Daten weisen eine normale oder rechtsschiefe Verteilung auf. Die rechtsschiefe Verteilung kann als Hinweis einer Anspruchsinflation und somit als eine „Überschätzung" des entsprechenden Items interpretiert werden. Betreffende Items wurden an die NV transformiert[30], damit anschliessend die explorative Faktorenanalyse gerechnet werden kann. Die Datenanalyse wurde im Programm SPSS Statistics 19 durchgeführt.

Bevor aber in die Analyse eingestiegen werden kann, wird mittels **Kaiser-Meyer-Olkin-Kriterium** (KMO) sowie des **Bartlett-Tests** geprüft, ob der Datensatz für die Durchführung einer Faktorenanalyse geeignet ist (Tabelle 2). Unter Voraussetzung normalverteilter Daten untersucht der Bartlett-Test, inwiefern die Stichprobe aus einer Grundgesamtheit entstammt, in der die Variablen unkorreliert sind (Backhaus, 2011; Dziuban & Shirkey, 1974). Da dieser Test bei grösseren Stichproben fast immer zu einem signifikanten Ergebnis führt (Signifikanz von .000), gilt er nur bei kleinen Fallzahlen als ausreichend und deshalb wurde zusätzlich das KMO-Kriterium gerechnet. In der Literatur wird das KMO-Kriterium als das beste zur Verfügung stehende Verfahren zur Überprüfung der Eignung des Datensatzes und somit der Korrelationsmatrix angesehen (Eckey, Kosfeld & Rengers, 2002; Dziuban & Shirkey, 1974). Der Test zeigt, ob eine Faktorenanalyse sinnvoll ist oder nicht. Ist der KMO < 0.5, ist der Datensatz nicht für eine Faktorenanalyse geeignet. Als wünschenswert sehen Kaiser und Rice (1974) ein KMO ≥ 0.8 an. Der KMO-Test im vorliegenden Da-

[30] Dieses Vorgehen ist damit zu begründen, dass bei einer starken Überschätzung des Items die Kategorien „wenig beachtet" und „nicht beachtet" nahezu identisch werden. Die Anpassung erfolgte durch eine Transformation (Potenzierung der Ursprungsdaten [x3-5]) und durch die Skalenkürzung (Skalenwerte 4 und 5 werden zusammengefasst).

tensatz ergab einen Wert von 0.969, das heisst, der Datensatz entspricht den Anforderungen einer Faktorenanalyse vollumfänglich (Backhaus et al., 2011).

Kaiser-Meyer-Olkin-Kriterium		**.969**
Bartlett-Test auf Sphärizität	Ungefähres Chi-Quadrat	40636.156
	Freiheitsgrade (degrees of freedom, df)	820
	Signifikanzniveau	**.000**

Tabelle 2: Kaiser-Meyer-Olkin-Kriterium und Barlett-Test für die Auswertung der Vertrauensfaktoren

Um die Anzahl der Faktoren zu bestimmen, wurde das **Eigenwert-Kriterium** (> 1) angewandt (Tabachnick, 2007). Basierend auf den Eigenwerten in Tabelle 3 wurden sechs Faktoren extrahiert. Der sechste Faktor liegt mit 1.008 sehr nahe am Grenzwert von 1, ist jedoch noch hoch genug, um in die Berechnungen mit einzufliessen (Tabachnick, 2007).

Faktoren	**Eigenwert**	**Anteil erklärter Varianz**
Faktor 1	15.565	16.022
Faktor 2	3.733	15.009
Faktor 3	2.724	11.677
Faktor 4	2.158	10.331
Faktor 5	1.265	6.858
Faktor 6	1.008	4.621
∑		**64.518**

Tabelle 3: Explorative Faktorenanalyse für die Auswertung der Vertrauensfaktoren

Tabelle 3 zeigt darüber hinaus den **Anteil der erklärten Varianz pro Faktor.** In Summe erklären diese sechs Faktoren fast 65 % der Varianz der ursprünglich neuen Items, das heisst, fast 65 % einer Änderung des Vertrauens zum Geschäftsmodell-Anbieter können durch diese sechs Faktoren erklärt werden.

Faktoren	**Interpretation**	**Mittelwert**	**Standardabweichung**
Faktor 1	Reziprozität	2.310	1.088
Faktor 2	Marke & Design	1.968	.930
Faktor 3	Nutzerkontrolle	2.542	1.307
Faktor 4	Kundenservice	2.477	1.406
Faktor 5	Realweltbezug	3.224	1.714
Faktor 6	Empfehlungen	2.866	1.455

Tabelle 4: Absolute Mittelwerte Ø der Vertrauensfaktoren (Interpretation :1 „trifft zu“, 5 „trifft nicht zu“)

Tabelle 4 zeigt die absoluten Mittelwerte der sechs Vertrauensfaktoren, betrachtet über den gesamten Datensatz. Der Faktor Marke und Design (Faktor 2) wurde von den Probanden am stärksten beachtet (Ø 1.968), danach folgt der Faktor Reziprozität (Faktor 1, Ø 2.310). Die beiden Faktoren Kundenservice (Faktor 4, Ø 2.477) und Nut-

zerkontrolle (Faktor 3, Ø 2.542) liegen im neutralen Bereich, während Empfehlungen (Faktor 6, Ø 2.866) und insbesondere dem Realweltbezug (Faktor 5, Ø 3.224) im Gesamten eher weniger Beachtung geschenkt wurden. Die relativ hohe Standardabweichung deutet auf eine grosse Schwankung der Antworten hin.

Im Anschluss an die Bestimmung der Faktoren-Anzahl wurde die Faktorladungsmatrix nach dem Varimax-Verfahren rotiert (Anhang 7.4.5) (Backhaus et al., 2011). Ziel dieser Rotation ist es, dass die Variablen immer nur auf einen Faktor laden (Rinne, 2000). Es konnten keine Kreuzladungen (ein Item lädt gleichzeitig auf zwei Faktoren) zwischen den Items festgestellt werden, das heisst, die Faktoren laden eindeutig auf den jeweiligen Faktor. Dies weist auf eine eindeutige Ladungsstruktur hin (Langer, 1999). Zehn Items wurden von der Hauptkomponentenanalyse ausgeschlossen, da entweder die Extraktion[31] oder die Faktorladung[32] zu gering war[33]. Die Faktorladungen und die Extraktionswerte sind im Detail im Anhang 7.4.5 nachzuschlagen. Alle Items der jeweiligen Faktoren wiesen Ladungen > 0.5 auf. Durch die Faktorenanalyse konnten demnach sechs relevante Vertrauensfaktoren identifiziert werden: Reziprozität, Marke und Design, Nutzerkontrolle, Kundenservice, Realweltbezug und Empfehlungen. Diese Vertrauensfaktoren wurden aus der Theorie identifiziert und im praktischen Kontext validiert. Auf die Konstruktion und die Benennung dieser Faktoren wurde bei der qualitativen Befragung von Anbietern und Nutzern im Kapitel 3.1.1 sowie im Theoriekapitel 3.2.2 näher eingegangen. Der sechste Faktor Empfehlungen hat jedoch nur drei bestätigte Items und der Eigenwert in Tabelle 3 war bereits sehr nahe am Grenzwert. In den folgenden Auswertungen muss besonders darauf geachtet werden, ob es Sinn ergibt, den Faktor Empfehlungen in die weiteren Analysen miteinzubeziehen.

---

[31] Grenzwert Extraktion < 0.5 (Backhaus et al., 2011).

[32] Grenzwert und Interpretation Faktorladung (auch Ladungskoeffizient genannt): Der Wertebereich liegt zwischen +1 und –1 und sagt aus, dass der Faktor positiv/negativ mit den Items korreliert. Bei einer Faktorladung von 0 sind der Faktor und die Items voneinander unabhängig. Eine Faktorladung von 1 bedeutet, dass der Faktor vollständig mit den Items korreliert und somit identisch ist (Langer, 1999). In der Literatur werden unterschiedliche Empfehlungen für den Grenzwert genannt: Chruchill (1991) schlagen > 0.3 vor; Homburg & Giering (1996) empfehlen > 0.4; Stewart (1981) setzt den Wert bei > 0.6 an. Aufgrund der hohen Fallzahl wird der Grenzwert der Faktorladung auf > 0.5 festgesetzt.

[33] Darunter befanden sich auch die Items des 7. Faktors „Technik“. Dieser konnte nur schlecht extrahiert werden (Faktorladung und Extraktion < 0.5) und musste deshalb aus den Berechnungen ausgeschlossen werden.

Vergleicht man dieses Ergebnis mit den Erkenntnissen aus der Theorie und den qualitativen Interviews (Abbildung 33), fällt auf, dass sich lediglich sechs der anfänglich vorgeschlagenen neun Faktoren durch die quantitative Analyse abbilden lassen. Der Faktor technische Zuverlässigkeit hat sich nicht bestätigt, Items des angedachten Faktors proaktive Kommunikation sind in den Faktor Reziprozität eingeflossen und die Faktoren Marke und Design wurden zusammengefasst.

Das **Cronbachs Alpha** berechnet die durchschnittliche Korrelation zwischen den Items (Eckey et al., 2002). Cronbachs Alpha wurde für jeden Faktor berechnet, um die Zuverlässigkeit der Messung festzustellen – dieser Wert liegt für alle Faktoren deutlich über dem Grenzwert von 0.6 (Peterson, 1994)[34] (Anhang 7.4.5) und bestätigt die Reliabilität der vorgenommenen Messung. Es scheint, dass der gewählte Forschungsansatz mit den qualitativen Interviews zur hohen Validität beitrug.

Faktorenanalyse des Vertrauensmasses: Vertrauen selbst ist auch wieder ein Konstrukt (also ein Faktor) und muss daher anhand verschiedener Items gemessen werden. Für die Reduktion aller Items auf dahinterstehende Faktoren wird erneut eine explorative Faktorenanalyse durchgeführt. Die Eignung des Datensatzes wurde wiederum mittels Kaiser-Meyer-Olkin-Kriterium (KMO .917 > 0.8) sowie Barlett-Test (Signifikanzniveau von .000) geprüft (Tabelle 5). Die explorative Faktorenanalyse ist durchführbar, da die Korrelationen nicht zufällig vorliegen (Kaiser & Rice, 1974).

Kaiser-Meyer-Olkin-Kriterium		**.917**
Bartlett-Test auf Sphärizität	Ungefähres Chi-Quadrat	20640.124
	Freiheitsgrade (degrees of freedom, df)	210
	Signifikanzniveau	**.000**

Tabelle 5: Kaiser-Meyer-Olkin-Kriterium und Barlett-Test für die Messung des Vertrauensmasses

Das Eigenwert-Kriterium (> 1) bestimmt die Anzahl Faktoren (Tabachnick, 2007). Die Faktorenanalyse (Tabelle 6) ergab, dass die operationalisierten Items auf vier Vertrauensfaktoren reduziert werden können:

[34] Grenzwerte Cronbachs Alpha: > 0,9 sehr gut, > 0,7 gut, > 0,6 akzeptabel, < 0,6 ist keine reliable Messung. Peterson (1994) erstellte in einer Studie eine Übersicht über die unterschiedlich verwendeten Grenzwerte des Cronbachs Alpha.

Faktoren	Eigenwert	Anteil erklärter Varianz
Faktor 1	5.754	27.400
Faktor 2	3.227	15.365
Faktor 3	3.172	15.104
Faktor 4	2.288	10.895
∑		68.764

Tabelle 6: Explorative Faktorenanalyse für die Messung des Vertrauensmasses

Das Vertrauensmass setzt sich aus vier Faktoren zusammen. Die Summe der erklärten Varianz liegt bei knapp 69 %. Es konnten keine Kreuzladungen zwischen den Items festgestellt werden (Anhang 7.4.6), die Faktoren laden also alle auf nur einen einzelnen Faktor (Langer, 1999). Die Faktorladungen und Extraktionswerte der einzelnen Items sind detailliert im Anhang 7.4.7 aufgeführt. Die Zuverlässigkeit der Messung wurde durch das Cronbachs Alpha (> 0.6) gemessen und die Ergebnisse zeigen alle eine hohe Messqualität.

Faktoren	Interpretation	Mittelwert	Standardabweichung
Faktor 1	Vertrauen in den Anbieter	2.018	.932
Faktor 2	Vertrauensneigung	2.736	.917
Faktor 3	Vertrauen in die Institution	2.832	1.063
Faktor 4	Vertrauensabsicht	1.604	.776

Tabelle 7: Absolute Mittelwerte Ø des Vertrauensmasses (Interpretation: 1 „trifft zu“, 5 „trifft nicht zu“)

Die absoluten Mittelwerte des Vertrauensmasses (Tabelle 7), gemessen über den gesamten Datensatz, zeigen eine stark positive Tendenz bei der Vertrauensabsicht (Ø 1.604), eine eher positive Tendenz bei Vertrauen in den Anbieter (Ø 2.018) sowie eher neutrale Tendenzen bei der Vertrauensneigung (Ø 2.736) und dem Vertrauen in die Institution (Ø 2.832). Das Vertrauensmass setzt sich demnach aus den vier Faktoren Vertrauen in den Anbieter, Vertrauensneigung, Vertrauen in die Institution und Vertrauensabsicht zusammen.

Im nachfolgenden Kapitel 3.1.5 werden die zentralen Erkenntnisse der Vorarbeiten nochmals zusammengefasst.

3.1.5 Zusammenfassung der Vorarbeiten

Dieses Kapitel war den Vorarbeiten für die forschungsmethodische Hauptuntersuchung gewidmet. Zuerst wurde der quantitative Fragebogen aus der Literaturrecherche und den qualitativen Interviews mit Anbietern und Nutzern von Online-Geschäftsmodellen hergeleitet. Der quantitative Fragebogen wurde an 11'846 in Deutschland wohnhafte Internetnutzer als Link per E-Mail verteilt und 1'549 Personen nahmen an der Umfrage teil. Gemäss KMO-Test ist der Datensatz für eine Faktorenanalyse sehr gut geeignet. Die 50 Items wurden mittels Faktorenanalyse zu sechs relevanten Vertrauensfaktoren verdichtet, wie in Abbildung 36 zusammengefasst:

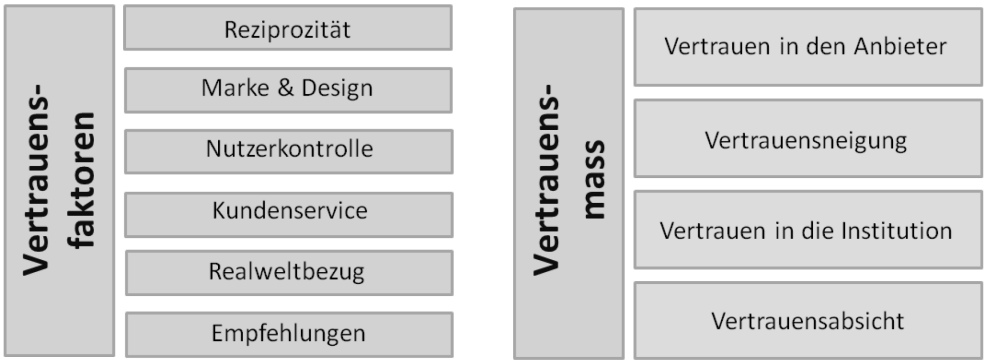


Abbildung 36: Zusammenfassung der Vertrauensfaktoren und des Vertrauensmasses (eigene Darstellung)

Ausserdem konnte durch eine zweite explorative Faktorenanalyse aufgezeigt werden, dass sich das Vertrauensmass aus den vier Faktoren Vertrauen in den Anbieter, Vertrauensneigung, Vertrauen in die Institution und Vertrauensabsicht zusammensetzt (Abbildung 36). Diese Ergebnisse werden in der Hauptuntersuchung im nächsten Kapitel aufgegriffen.

3.2 Hauptuntersuchung

In diesem Kapitel werden die methodischen Verfahren vorgestellt, durchgeführt und erläutert, um die in Kapitel 1.2.1 definierten Forschungsfragen zu beantworten. Für die Identifikation der Vertrauenstypen werden im Kapitel 3.2.1 die Clusteranalyse und die Diskriminanzanalyse vorgestellt. Sowohl für die Identifikation der relevanten Vertrauensfaktoren im Kapitel 3.2.2 als auch für die Identifikation der Vertrauensabsichten pro Vertrauenstyp im Kapitel 3.2.3 wird ein Mittelwertvergleich angewendet.

3.2.1 Identifikation von Vertrauenstypen

Unterschiedliche Vertrauenstypen haben ein differenziertes Vorschussvertrauen und gehen damit anders in die jeweilige Situation hinein. Vertrauen im Online-Bereich kann davon abhängen, wie schnell Menschen im realen Leben Drittparteien vertrauen oder misstrauen. Rotter (1967) argumentiert, dass Vertrauen erlernbar ist und dass Vertrauen ein Persönlichkeitsmerkmal darstellt – ein gewisses Mass an Vertrauen bringt demnach jede Person in eine Situation mit ein. Deshalb wird bei der Identifikation von unterschiedlichen Vertrauenstypen im Internet eine Ex-ante-Betrachtung herangezogen. Um die erste Forschungsfrage „Existieren bei Internetnutzern unterschiedliche Vertrauenstypen?“ beantworten zu können, wird die Methodik der Clusteranalyse angewendet. Diese geht der Frage nach, ob zwischen den betrachteten Untersuchungsobjekten Ähnlichkeiten bestehen, um diese zu einer möglichst homogenen Gruppe (Cluster) zusammenzufassen. Untereinander sollten die Gruppen jedoch eine möglichst grosse Heterogenität aufweisen (Bacher, Pöge & Wenzig, 2010). Die Clusteranalyse gehört zu den explorativen Verfahren der multivarianten Datenanalyse, da die Gruppen zu Beginn der Analyse unbekannt sind (es werden neue Gruppen gebildet) und diese erst mithilfe des Clusterverfahrens ermittelt werden (Backhaus et al., 2011).

In diesem Kapitel soll untersucht werden, ob sich die Erhebungsgesamtheit in unterschiedliche Vertrauenstypen gliedern lässt, wobei als Merkmalsvariablen die drei in der vorhergehenden Faktorenanalyse identifizierten Ex-ante-Vertrauensfaktoren herangezogen werden: das **Vertrauen in den Anbieter,** die **Vertrauensneigung** so-

wie das **Vertrauen in die Institution**[35]. Ein wesentliches Merkmal der Clusteranalyse ist es, dass alle Merkmalsvariablen gleichzeitig zur Gruppenbildung herzangezogen werden (Backhaus et al., 2011).

Für die Durchführung einer Clusteranalyse bestehen keine Voraussetzungen, auf welche die Daten im Vorfeld geprüft werden müssen (Backhaus et al., 2011). Der Ablauf einer Clusteranalyse lässt sich gemäss Backhaus et al. (2011) in drei grundlegende Schritte unterteilen: Bestimmung der Ähnlichkeiten bzw. Distanzen, Auswahl des Fusionierungsalgorithmus sowie die Bestimmung der optimalen Clusterzahl, wie in Abbildung 37 grafisch dargestellt.

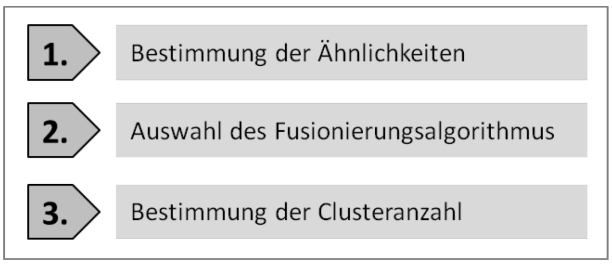


Abbildung 37: Ablaufschritte der Clusteranalyse (eigene Darstellung in Anlehnung an Backhaus et al., 2011)

Bestimmung der Ähnlichkeiten bzw. Distanzen: Um die Ähnlichkeiten oder die Distanzen zu eruieren, werden für jeweils zwei Objekte die Ausprägungen der Merkmalsvariablen geprüft und die Unterschiede (Distanzfunktion zur Bestimmung des Abstandes) bzw. Übereinstimmungen (Ähnlichkeitsfunktion zur Bestimmung der Ähnlichkeit) durch das Proximitätsmass gemessen. Die Distanz ist die Unähnlichkeit der Merkmalsvariablen, das bedeutet, je unähnlicher, je grösser die Distanz zwischen den Variablen und je grösser der Ähnlichkeitswert zwischen zwei Objekten, desto ähnlicher sind sie sich (Backhaus et al., 2011). Die Merkmalsvariablen werden zuerst einzeln verglichen und aus den kumulierten Distanzen bzw. Ähnlichkeiten wird die Gesamtdistanz oder -ähnlichkeit errechnet (Bacher et al., 2010). Die einzeln errechneten Distanzen bzw. Ähnlichkeiten werden Proximität genannt, die kumulierten Distanzen werden in einer Proximitätsmatrix (auch Distanztabelle oder Distanzmatrix genannt) zusammengefasst, welche jeweils zwei Merkmalen eine Proximität zuweist (Deichsel & Trampisch, 1985; Backhaus et al., 2011). Operationalisiert bedeutet dies, dass die Rohdatenmatrix im SPSS in die Proximitätsmatrix überführt

[35] Der vierte Faktor Vertrauensabsicht des Vertrauensmasses ist eine Ex-post-Betrachtung von Vertrauen und wird bei der Forschungsfrage 3 im Kapitel 3.2.3 herangezogen.

wird, welche immer eine quadratische Matrix darstellt. Um die Proximität zu messen, stehen dem Forscher drei Hauptkategorien von Skalen (möglicher Wertebereich der Merkmalsvariablen) zur Verfügung (Deichsel & Trampisch, 1985): binäre, nominale und metrische Skalen.[36] Der Fragebogen für die Online-Umfrage (Anhang 7.4.1) wurde grösstenteils anhand metrischer Skalen konzeptioniert und deshalb wird die Ähnlichkeit anhand der metrischen Variablenstruktur ermittelt. Die quadrierte euklidische Distanz ist ein weit verbreitetes metrisches Distanzmass, welches die Trennung der Merkmalsvariablen klar herausarbeitet (Backhaus et al., 2011)[37]. Das Distanzmass prüft für jeweils zwei Objekte die Ausprägungen der Beschreibungsmerkmale. Durch die Quadratisierung werden geringere Abweichungen verhältnismässig unwichtiger, während grössere Abweichungen sehr stark ausgeprägt werden. Dies führt zu einer starken Gruppenbildung, indem Merkmalsvariablen entweder aneinandergeschweisst oder auseinandergerissen werden. Aufgrund dieser starken Trennkraft wird in dieser Arbeit die quadrierte euklidische Distanz für die Bestimmung der Unähnlichkeiten verwendet. Die in der Distanzmatrix (Matrix der euklidischen Distanzen) angegebenen Unähnlichkeitswerte wurden nach der allgemeinen Formel der euklidischen Distanz im SPSS berechnet.

Auswahl des Fusionierungsalgorithmus: Die vorher erstellte Distanzmatrix bildet nun den Ausgangspunkt für die Auswahl des Fusionierungsalgorithmus. Um den Fusionierungsalgorithmus zu bestimmen, werden die Distanzwerte so zu Gruppen zusammengefasst (die Proximitätsmatrix wird reduziert), dass sich diejenigen Objekte in einer Gruppe wiederfinden, welche möglichst übereinstimmende Merkmalsvariablen aufweisen. Entsprechend der Vorschriften des Fusionierungsalgorithmus fasst die Clusteranalyse die Fälle so lange zusammen, bis alle in einer Gruppe enthalten sind (Backhaus et al., 2011). Die Auswahl möglicher zu verwendender Cluster-Algorithmen wird im Anhang 7.5.1 in der Abbildung 95 ausführlich disku-

[36] Binäre Skalen: Die Merkmalsvariable kann zwei Werte annehmen, z. B. 0 für männlich und 1 für weiblich. Nominale Skalen: Die Merkmalsvariable kann unterschiedliche Werte annehmen, um eine qualitative Unterscheidung zu treffen (Häufigkeiten), z. B. Geburtsort. Metrische Skalen: Die Merkmalsvariable nimmt einen Wert auf einer vorher festgelegten Skala an (Intervall), um eine quantitative Aussage zu treffen, z. B. Likert-Skala 1 bis 5.

[37] In Abhängigkeit des betrachteten Skalenniveaus existiert eine Vielzahl an Proximitätsmassen, zur Verfügung stehen zum Beispiel die Minkowski-Metriken oder die L-Normen (City-Block-Metrik), die einfache und quadrierte euklidische Distanz sowie der Q-Korrelationskoeffizient (Backhaus et al., 2011). Viele der Masse sind gegeneinander austauschbar (Brosius, 2008).

tiert. Für die Analyse der Distanzmatrix wird das weit verbreitete Ward-Verfahren herangezogen. Vorteil dieses Verfahrens ist, dass Gruppen mit gleicher Gruppenstärke gebildet werden, die gut miteinander verglichen werden können, und dass die Objekte richtig den Gruppen zugeordnet werden (Bergs, 1981). Ein Nachteil ist, dass Ausreisser das Ergebnis der Clusterbildung verwässern. Dieser Datensatz weist jedoch keine Ausreisser auf, weshalb das Ward-Verfahren angewendet werden kann. Weitere Voraussetzungen sind, dass alle Variablen auf metrischem Skalenniveau gemessen wurden (Likert-Skala 1–5 angewandt) und dass die Variablen unkorreliert sind (durch vorhergehende Faktorenanalyse sichergestellt).

Solange noch keine Objekte vereinigt wurden, bestehen noch genauso viele Gruppen wie Objekte. Das Ziel des Ward-Verfahrens ist es, diejenigen Gruppen zu vereinigen, die die Streuung (Varianz) in einer Gruppe möglichst wenig erhöhen (Varianzkriterium oder Fehlerquadratsumme genannt), wodurch vergleichsweise homogene Cluster gebildet werden. Deshalb wird dieses Verfahren auch Minimum-Varianz-Verfahren genannt. Dem Ward-Verfahren liegt als Proximitätsmass die quadrierte euklidische Distanz zugrunde; somit basiert es auf der bereits errechneten Distanzmatrix. Um den Fusionierungsalgorithmus zu bestimmen, werden die Distanzwerte so zu Gruppen zusammengefasst (die Proximitätsmatrix wird reduziert), dass sich diejenigen Objekte in einer Gruppe wiederfinden, welche möglichst übereinstimmende Merkmalsvariablen aufweisen. Im ersten Schritt werden je zwei Variablen einer Gruppe zugeordnet, welche möglichst ähnlich sind bzw. welche das vorgegebene Heterogenitätsmass am wenigstens vergrössern. Mit den neuen Gruppen wird die Distanzmatrix nochmals neu gerechnet und wieder werden jeweils zwei Gruppen einer Gruppe zugeordnet usw. Dieser Prozess wird so lange wiederholt, bis nur noch eine Gruppe besteht. Im Anhang 7.5.2 ist ein Einblick in die Zuordnungsübersicht anhand des Ward-Verfahrens abgebildet. Grafisch dargestellt wird das Ergebnis des Verfahrens mittels Dendrogramm (Anhang 7.5.3).

Bestimmung der optimalen Clusterzahl: Es ist wichtig zu bestimmen, wie viele Cluster tatsächlich gebildet werden sollen, denn der Fusionierungsalgorithmus würde so lange fusionieren, bis nur noch eine einzige Gruppe vorhanden ist. Ziel dieser Arbeit ist es, unterschiedliche Vertrauenstypen zu identifizieren und nicht alle Personen einem Typ zuzuordnen. Wann aber sollte die Zuteilung in Gruppen unterbrochen werden? Die optimale Clusterzahl wird durch die Betrachtung der Varianz innerhalb und zwischen den Gruppen bestimmt. Dabei muss zwischen der Handhabbarkeit (geringe Clusterzahl) und der Homogenitätsanforderung (grosse Clusterzahl)

abgewogen werden (Backhaus et al., 2011). Das Elbow-Kriterium liefert eine optische Identifikation eines Sprungs in der Veränderung des Heterogenitätsmasses alternativer Clusterlösungen. Bildet sich ein klar ersichtlicher Knick, ist dies das Entscheidungskriterium für die zu wählende Clusterzahl. Gemäss Elbow-Kriterium ist folglich eine Drei-Cluster-Lösung zu wählen (Abbildung 38). [38]

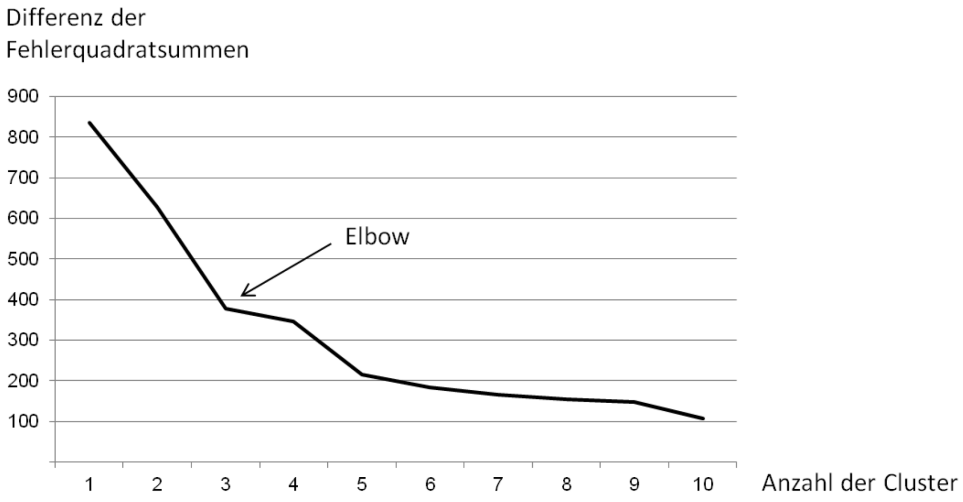


Abbildung 38: Elbow-Kriterium zur Bestimmung der optimalen Clusterzahl (eigene Darstellung)

Wie in Tabelle 8 ersichtlich, wurden mithilfe des Ward-Verfahrens dem ersten Vertrauenstyp 524 Personen (34 %), dem zweiten Vertrauenstyp 526 Personen (34 %) und dem dritten Vertrauenstyp 499 Personen (32 %) zugeordnet, die Gruppen sind demnach ungefähr gleich gross.

Ward-Verfahren		Vertrauen in den Anbieter	Vertrauens-neigung	Vertrauen in die Institution
Vertrauenstyp 1	Mittelwert	1.0234169	.0506844	-.0734210
(n = 524)	Std.-Abw.	.67811201	1.01365896	.94100209
Vertrauenstyp 2	Mittelwert	-.6464492	.3412389	-.6189341
(n = 526)	Std.-Abw.	.54826264	1.06070213	.76253506
Vertrauenstyp 3	Mittelwert	-.3932629	-.4129264	.7295229
(n = 499)	Std.-Abw.	.78115355	.73940190	.78863782
Total	Mittelwert	.0000000	.0000000	.0000000
(n = 1'549)	Std.-Abw.	1.00000000	1.00000000	1.00000000

Tabelle 8: Analyse der Vertrauenstypen anhand des relativen Mittelwertes (Interpretation: negative Werte tendieren zu „trifft zu", positive Werte zu „trifft nicht zu")

[38] Berechnungsbeispiel Elbow-Grafik: Der Zuordnungsübersicht im Anhang 7.5.2 sind die letzten beiden errechneten Fehlerquadratsummen zu entnehmen: 4'644 und 3'808. Dies ergibt eine Differenz von 836 (Vergrösserung des Heterogenitätszuwachses und Anstieg der Fehlerquadratsumme), wie in Abbildung 38 ersichtlich.

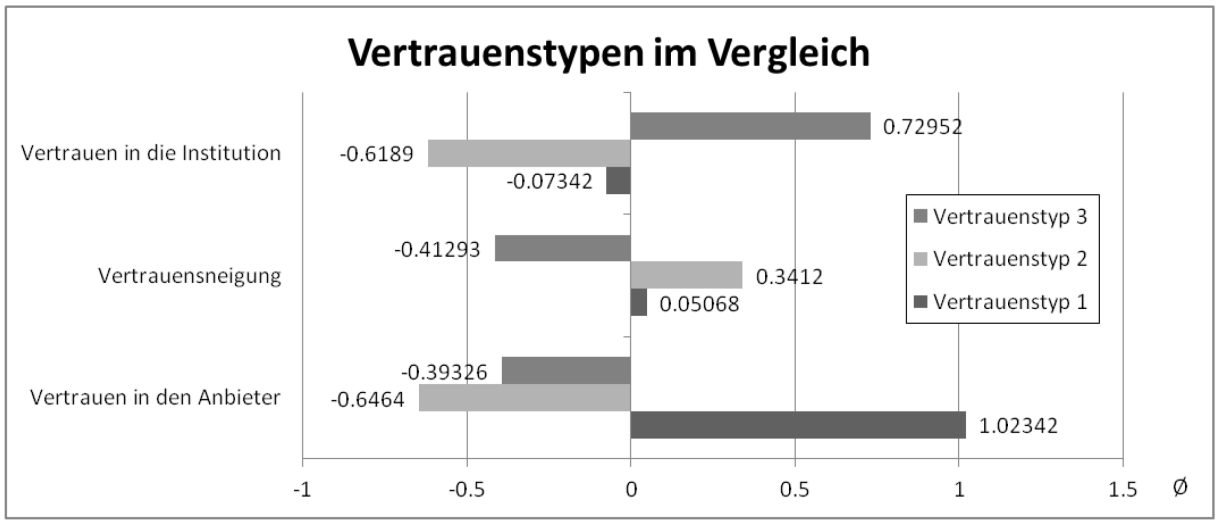


Abbildung 39: Vertrauenstypen anhand des relativen Mittelwertes (Interpretation: negative Werte tendieren zu „trifft zu", positive Werte zu „trifft nicht zu")

Erste Interpretation der Cluster: Nach der Bestimmung der optimalen Clusterzahl müssen die Cluster anhand des z-transformierten relativen Mittelwertes der für die Clusterung verwendeten Faktoren interpretiert werden (Tabelle 8 und Abbildung 39). Bei der Interpretation ist zu erwähnen, dass negative Abweichungen eine Tendenz in Richtung „trifft zu" und positive Werte eine Tendenz in Richtung „trifft nicht zu" im Vergleich zum gesamten Sample andeuten.

- Der **Vertrauenstyp 1** sticht im Vergleich zu den anderen beiden Gruppen durch sein niedriges Vertrauen in den Anbieter hervor (Ø 1.02) und hat mässiges Vertrauen in die Institution Internet (Ø -0.07). Auch die leicht positive Vertrauensneigung (Ø 0.05) deutet darauf hin, dass dieser Typ eher wenig Vertrauen gegenüber anderen Menschen hat. Es scheint, dass sich dieser Typ bei einer Transaktion nicht nur auf den Anbieter selbst verlässt.
- **Vertrauenstyp 2** weist im Vergleich ein hohes Mass an Vertrauen in den jeweiligen Anbieter (Ø -0.65) wie auch eine positive Vertrauenstendenz in die Institution Internet (Ø -0.62) auf. Im Vergleich zum Durchschnitt vertraut dieser Typ anderen Menschen eher weniger (Ø 0.34). Dieses Ergebnis könnte darauf hindeuten, dass Personen dieses Vertrauenstyps gegenüber dem Anbieter und Internettransaktionen im Allgemeinen eher positiv eingestellt sind.
- **Vertrauenstyp 3** zeichnet sich im Vergleich durch seine eher negative Vertrauenstendenz zur Institution Internet aus (Ø 0.73), hat aber tendenziell

Vertrauen in den jeweiligen Anbieter (Ø -0.39) und hat gegenüber den anderen Clustern höheres Vertrauen in andere Menschen (Ø -0.41). Es scheint, dass diese Personen dazu tendieren, dem Internet weniger zu vertrauen, sie verlassen sich eher auf den Anbieter und die Menschen.

Bevor im Kapitel 4.1 vertieft in die Interpretation der Ergebnisse der Clusteranalyse eingestiegen wird, wird die Güteprüfung der Clusteranalyse anhand der Diskriminanzanalyse vorgenommen.

Überprüfung der Güte der Clusteranalyse anhand einer Diskriminanzanalyse: Als Güteprüfung der Clusteranalyse empfehlen Backhaus et al. (2011) die Diskriminanzanalyse. Die Analyse wird eingesetzt, um Unterschiede in den Gruppen hinsichtlich der Variablen zu untersuchen (Trennschärfe der Gruppen zu bestimmen) sowie die Gruppenstabilität zu testen. Nach Durchführung der Diskriminanzanalyse kann beantwortet werden, ob sich die Vertrauenstypen signifikant voneinander unterscheiden und welche Variablen zur Unterscheidung zwischen den Vertrauenstypen geeignet sind.

Die Unterscheidung der Vertrauenstypen wird anhand der zuvor einbezogenen Vertrauensfaktoren (Vertrauen in den Anbieter, Vertrauensneigung und Vertrauen in die Institution) untersucht. Neben der Analyse der Gruppenunterschiede soll durch die Diskriminanzanalyse auch eine Prognose über die Gruppenzugehörigkeit berechnet werden (Backhaus et al., 2011).

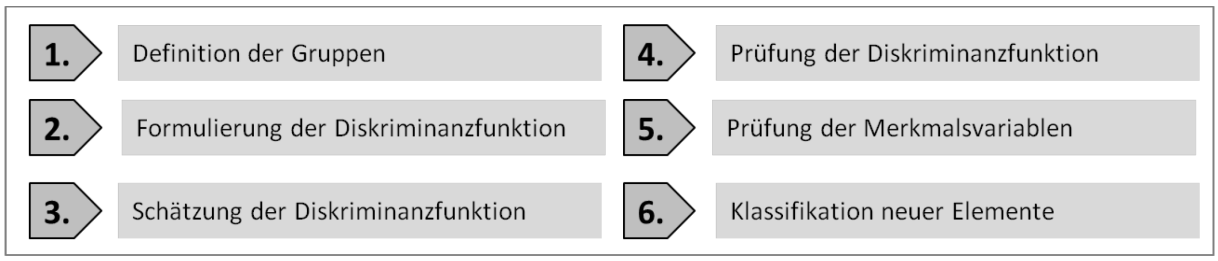


Abbildung 40: Ablaufschritte der Diskriminanzanalyse (eigene Darstellung in Anlehnung an Backhaus et al., 2011)

Die Vertrauenstypen wurden bereits durch die Clusteranalyse definiert, der erste Schritt, die Definition der Gruppen (Abbildung 40), entfällt daher für die Güteprüfung. Die Diskriminanzfunktion[39] ermöglicht eine optimale Trennung der Cluster

[39] Diskriminanzfunktion $Y = b0 + b1X1 + b2X2 + \ldots + bjXj$

und prüft die diskriminatorische Bedeutung der einzelnen Merkmalsvariablen (Vertrauen in den Anbieter, Vertrauensneigung und Vertrauen in die Institution). Durch die Differenz der mittleren Diskriminanzwerte (Centroid) der einzelnen Gruppen kann die Unterschiedlichkeit festgestellt werden. Die Diskriminanzfunktion soll so geschätzt werden, dass sie optimal zwischen den untersuchten Gruppen trennt (Backhaus et al., 2011). Da drei Cluster bestehen, können zwei Diskriminanzfunktionen ermittelt werden.

Anhand der Eigenwerte und des residuellen Wilks' Lambda wird die Güteprüfung für die Diskriminanzfunktion vollzogen. Die Diskriminanzfunktion sollte einen wesentlichen Erklärungswert aufweisen. Als Gütekriterium für die relative Wichtigkeit einer Diskriminanzfunktion wird der Eigenwertanteil (erklärter Varianzanteil) verwendet (Backhaus et al., 2011). Zu jeder Diskriminanzfunktion gehört ein Eigenwert, der den Maximalwert des Diskriminanzkriteriums ermittelt. Wie in Tabelle 9 abgebildet, weisen die beiden Funktionen einen wesentlichen Eigenwertanteil (> 0) auf und können deshalb für die Analyse verwendet werden.[40]

Funktion	Eigenwert	Kanonischer Korrelationskoeffizient
1	1.216*	.741
2	.658*	.630

Tabelle 9: Eigenwert zur Prüfung der Diskriminanzfunktionen
(Die zwei ersten kanonischen Diskriminanzfunktionen wurden in der Analyse verwendet.)*

Gemäss Backhaus et al. (2011) bildet Wilks' Lambda das gebräuchlichste Kriterium zur Prüfung der Diskriminanz. Tabelle 10 zeigt den Wert für das residuelle Wilks' Lambda für die Diskriminanzfunktionen an. Er gibt Auskunft darüber, ob die Einbeziehung einer weiteren Diskriminanzfunktion die Gruppentrennung noch verbessert. Es ist zu erkennen, dass auch die zweite Diskriminanzfunktion noch signifikant zur Trennung der Gruppen beiträgt.

Y = Diskriminanzvariable; X_j = Merkmalsvariable j; b_j = Diskriminanzkoeffizient für Merkmalsvariable j; b_0 = konstantes Glied

[40] Der kanonische Korrelationskoeffizient ist ein Mass für die wechselseitige Abhängigkeit zweier Gruppen und liegt im Bereich von 0.6 bis 0.7 (Grenzwert > 0.5) (Backhaus et al., 2011), was bedeutet, dass die Gruppen signifikant voneinander abhängig sind.

Funktionstest	Wilks' Lambda	Signifikanz
1 bis 2	.272	.000
2	.603	.000

Tabelle 10: Wilks' Lambda zur Prüfung der Diskriminanzfunktionen

Um die Frage zu beantworten, wie gut die Merkmalsvariablen für die Clusteranalyse geeignet sind, werden die Merkmalsvariablen auf Gleichheit der Mittelwerte hin getestet. Das univariate Wilks' Lambda gibt den Anteil der nicht erklärten Streuung an der Gesamtstreuung an (Tabelle 11).

	Wilks' Lambda	Signifikanz
Vertrauen in den Anbieter	.454	.000
Vertrauensneigung	.905	.000
Vertrauen in die Institution	.696	.000

Tabelle 11: Prüfung der Merkmalsvariablen

Kleinere Werte bedeuten eine höhere Trennkraft der Merkmalsvariablen (Backhaus et al., 2011). Die beste Trennkraft besitzt demnach die Variable „Vertrauen in den Anbieter". Alle Variablen besitzen signifikante Trennkraft und können demnach für die Trennung der drei Vertrauenstypen verwendet werden.

Interpretation der Diskriminanzfunktion anhand der standardisierten Diskriminanzkoeffizienten: Wie in Tabelle 12 ersichtlich, kommt die grösste diskriminatorische Bedeutung der Variable „Vertrauen in den Anbieter" für die Funktion 1 und der Variable „Vertrauen in die Institution" für die Funktion 2 zu.

	Funktion 1	Funktion 2
Vertrauen in den Anbieter	.995	-.105
Vertrauensneigung	-.074	-.596
Vertrauen in die Institution	.136	.930

Tabelle 12: Standardisierte Diskriminanzkoeffizienten

Werden die Merkmalsvariablen mit dem Eigenwert der jeweiligen Funktion gewichtet, sind die mittleren Diskriminanzkoeffizienten berechenbar[41]:

[41] Mittlerer Diskriminanzkoeffizient = Koeffizient F1 * Eigenwert F1 + Koeffizient F2 * Eigenwert F2

Vertrauen in den Anbieter = 0.995 * 1.216 + 0.105 * 0.658 = 1.36829

Vertrauensneigung = 0.074 * 1.216 + 0.596 * 0.658 = 0.482152

Vertrauen in die Institution = 0.136 * 1.216 + 0.930 * 0.658 = 0.777316

Die Merkmalsvariable mit der grössten diskriminatorischen Bedeutung ist wiederum „Vertrauen in den Anbieter“ (siehe auch Tabelle 11) gefolgt von „Vertrauen in die Institution“. Die Variable „Vertrauensneigung“ hat die geringste diskriminatorische Bedeutung.

Interpretation anhand der Klassifizierungsfunktion: Als Beispiel für die Interpretation wird Proband Nr. 1 (Laufnummer 2334 im Datensatz) anhand der Klassifizierungsfunktion den drei Vertrauenstypen zugeteilt. Der Proband Nr. 1 besitzt gemäss Datensatz die Faktorenwerte 1.089 (Vertrauen in den Anbieter), 0.14251 (Vertrauensneigung) und 0.70961 (Vertrauen in die Institution).

	Ward-Methode		
	Vertrauenstyp 1	Vertrauenstyp 2	Vertrauenstyp 3
Vertrauen in den Anbieter	2.250	-1.472	-.811
Vertrauensneigung	.055	.586	-.675
Vertrauen in die Institution	-.060	-1.069	1.190
Konstant	-2.254	-2.005	-1.832

Tabelle 13: Fishers lineare Klassifizierungsfunktion

Diese Werte werden nun in die Klassifizierungsfunktion (Matrix in Tabelle 13) eingesetzt, um Proband Nr. 1 exemplarisch einem Vertrauenstyp zuordnen zu können. Der Proband wird demjenigen Vertrauenstyp zugeordnet, bei welchem die Funktion ihren grössten Wert annimmt (bei der sie maximal wird):

Vertrauenstyp 1 = 2.250 * 1.089 + 0.055 * 0.14251 - 0.060 * 0.70961 - 2.254 = 0.16151145

Vertrauenstyp 2 = -1.472 * 1.089 + 0.586 * 0.14251 - 1.069 * 0.70961 - 2.005 = -4.28307023

Vertrauenstyp 3 = -0.811 * 1.089 - 0.675 * 0.14251 + 1.190 * 0.70961 - 1.832 = -1.96693735

Der Proband Nr. 1 würde demnach dem Vertrauenstyp 1 zugeordnet werden. Dieses Resultat bestätigt die Clusteranalyse.

Interpretation anhand der Klassifizierungsergebnisse: Die Clusteranalyse teilte 524 Probanden dem Vertrauenstyp 1 zu, die Diskriminanzanalyse hingegen nur 445 Personen. 41 Probanden wurden „fälschlicherweise“ dem Vertrauenstyp 2 und 38 dem Vertrauenstyp 3 zugeordnet (Tabelle 14). Die Trefferquote der Diskriminanzanalyse in der Untersuchungsstichprobe beträgt 82.3 %. Dies ist ein sehr zufriedenstellendes Ergebnis, das besagt, die drei Typen wurden sehr treffend klassifiziert. Die

Interpretation anhand der Klassifizierungsergebnisse zeigt, dass die Gütekriterien erfüllt sind und die Ergebnisse der Clusteranalyse und die Trennung der Cluster gültig und für weitere Analysen nutzbar sind.

	Ward-Methode		Erwartete Gruppenzugehörigkeit			
			Vertrauens-typ 1	Vertrauens-typ 2	Vertrauens-typ 3	Total
Original	Anz.	Vertrauenstyp 1	**445**	41	38	524
		Vertrauenstyp 2	30	**452**	44	526
		Vertrauenstyp 3	63	58	**378**	499
Original	%	Vertrauenstyp 1	**84.9**	7.8	7.3	100.0
		Vertrauenstyp 2	5.7	**85.9**	8.4	100.0
		Vertrauenstyp 3	12.6	11.6	**75.8**	100.0

Tabelle 14: Klassifizierungsergebnisse (die Trefferquote beträgt 82.3 %)

Durch Gegenüberstellung der Funktionswerte lassen sich die Klassifizierungsergebnisse auch grafisch darstellen. Abbildung 41 zeigt die Gruppenzentren der drei Vertrauenstypen. Diejenigen Werte, welche im Zentrum liegen, wurden zu 100 % richtig geschätzt. Hier wird optisch ersichtlich, dass die geschätzten Werte sehr nah an den Zentren liegen und sich die Gruppen nicht überschneiden.

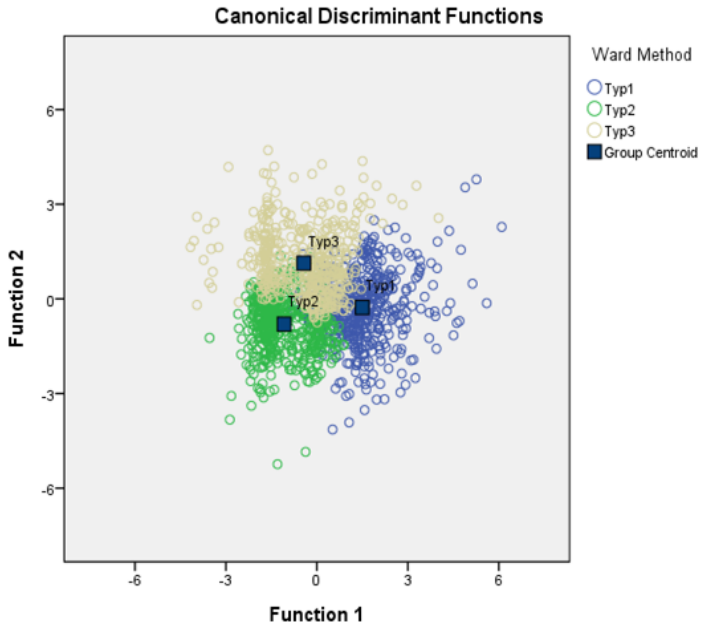


Abbildung 41: Grafische Darstellung der Vertrauenstypen im Diskriminanzraum (SPSS Output)

In diesem Kapitel wurden durch eine Clusteranalyse aufgrund der Merkmalsvariablen Vertrauen in den Anbieter, Vertrauensneigung und Vertrauen in die Institution drei unterschiedliche Vertrauenstypen identifiziert. Im folgenden Kapitel wird un-

tersucht, ob für die drei Vertrauenstypen während einer Transaktion unterschiedliche Vertrauensfaktoren relevant sind.

3.2.2 Relevante Vertrauensfaktoren pro Vertrauenstyp

In den forschungsmethodischen Vorarbeiten wurden mittels Faktorenanalyse die folgenden sechs Vertrauensfaktoren identifiziert: Reziprozität, Marke und Design, Nutzerkontrolle, Kundenservice, Realweltbezug und Empfehlungen (Kapitel 3.1.4). Durch die Clusteranalyse im Kapitel 3.2.1 wurden drei unterschiedliche Vertrauenstypen im Internet identifiziert. Jetzt stellt sich die Frage, ob alle sechs identifizierten Vertrauensfaktoren während einer Transaktion (in situ) im Internet für jeden Vertrauenstyp gleich relevant sind oder ob die unterschiedlichen Typen auf andere Vertrauensindizien reagieren. Dies soll in diesem Kapitel mithilfe der zweiten Forschungsfrage „Sind während einer Transaktion im Internet für die unterschiedlichen Vertrauenstypen dieselben Vertrauensfaktoren relevant?“ beantwortet werden.

Anhand des Kruskal-Wallis-Tests (auch H-Test genannt) sollen nun signifikante Unterschiede zwischen den Vertrauenstypen hinsichtlich der sechs relevanten Vertrauensfaktoren identifiziert werden (Kruskal & Wallis, 1952). Diese Analyse testet Mittelwertunterschiede von ungleichen Gruppen (Hirsig, 2001), in diesem Fall die Mittelwerte der Vertrauensfaktoren. Die Varianz der Zielvariablen (abhängige Variablen: Vertrauensfaktoren) wird durch mehrere Einflussvariablen (unabhängige Variablen: Vertrauenstyp) erklärt. Um ein Mittelwertvergleich durchführen zu können, ist es wichtig, dass die Skalen metrisch sind. Dies ist gewährleistet, da es sich bei den Variablen um berechnete Faktorwerte handelt. Für Vertrauensfaktoren, die parametrisch (metrisch und normalverteilt) sind, bei denen aber keine Varianzgleichheit vorliegt, kann der Kruskal-Wallis-Test angewendet werden (Hirsig, 2001).

	Reziprozität	Marke & Design	Nutzerkontrolle	Kundenservice	Realweltbezug	Empfehlungen
Chi-Quadrat	121.135	117.603	9.578	96.1000	3.219	8.718
Asymp. Sig.	.000	.000	.008	.000	.200	.013

Tabelle 15: Kruskal-Wallis-Test der Vertrauensfaktoren (Kruskal Wallis Test / Grouping Variable: Ward-Method CLU3_1)

Wie in Tabelle 15 ersichtlich, unterscheiden sich die vier Vertrauensfaktoren Reziprozität, Marke und Design, Nutzerkontrolle und Kundenservice signifikant nach Typ (Signifikanz < .01). Die Vertrauensfaktoren Realweltbezug und Empfehlungen

unterscheiden sich nicht signifikant nach Typ und werden deshalb von den weiteren Analysen ausgeschlossen (Signifikanz > .01)[42].

Ward-Methode	Reziprozität	Marke & Design	Nutzerkontrolle	Kundenservice
Typ 1 Mittelwert (n = 524)	.3102399	.3703892	.0586255	.3095810
Typ 1 St.-Abweichung	.93543287	1.01926573	.95884494	.98975727
Typ 2 Mittelwert (n = 526)	-.2969286	-.2580064	-.0838097	-.2266687
Typ 2 St.-Abweichung	.98270787	.91467532	.97122251	.93970704
Typ 3 Mittelwert (n = 499)	-.0127881	-.1169791	.0267818	-.0861578
Typ 3 St.-Abweichung	.98835084	.95237317	1.06617436	.99305664
∑ Mittelwert (n = 1'549)	.0000000	.0000000	.0000000	.0000000
∑ St.Abweichung	1.00000000	1.00000000	1.00000000	1.00000000

Tabelle 16: Effektive Mittelwertabweichungen der Vertrauensfaktoren pro Vertrauenstyp (Interpretation: negative Werte tendieren zu „stark beachtet", positive Werte zu „nicht beachtet")

Tabelle 16 zeigt die Mittelwertabweichung der Vertrauensfaktoren pro Vertrauenstyp, um die Abweichung der Mittelwerte der Faktoren pro Vertrauenstyp diskutieren zu können. Die Werte müssen folgendermassen interpretiert werden: Negative Werte repräsentieren eine Tendenz zu „trifft zu" und positive Werte eine Tendenz zu „trifft nicht zu".

- **Vertrauenstyp 1** achtet im Vergleich zu den anderen Vertrauenstypen am wenigsten auf die getesteten Vertrauensfaktoren. Die Marke und das Design (Ø .370), das Reziprozitätsverhältnis (Ø .310) wie auch den Kundenservice (Ø .310) scheint er weniger zu beachten, genauso den Faktor Nutzerkontrolle (Ø .059).
- **Vertrauenstyp 2** achtet im Vergleich auf alle vier Vertrauensfaktoren. Besonders relevant ist für ihn die Reziprozität (Ø -.297) dicht gefolgt von Marke und Design (Ø -.258), danach folgt für ihn der Kundenservice (Ø -.227). Schlusslicht der Relevanz bildet die Nutzerkontrolle (-.084), die er tendenziell neutral betrachtet. Im Vergleich zu den anderen beiden Typen beachtet er alle Faktoren stärker.
- Auch **Vertrauenstyp 3** achtet besonders auf die Marke und das Design (Ø -.117) eines Anbieters. Zudem achtet er auf den Kundenservice (Ø -.086) und schwach auf das Reziprozitätsverhältnis (Ø -.018), im Vergleich aber unterdurchschnittlich auf die Nutzerkontrolle (Ø .027).

[42] Beim Faktor Empfehlungen könnte die Signifikanz mit 0.013 noch als keine Korrelationen interpretiert werden, in den vorhergehenden Analysen wurde jedoch bereits auf den geringen Eigenwert sowie die geringe Itemzahl des Faktors Empfehlungen hingewiesen und deshalb wird dieser Faktor nicht mehr weiter in die Analyse miteinbezogen.

Zusammenfassend zeigt Abbildung 42 die relevanten Vertrauensfaktoren pro Vertrauenstyp.

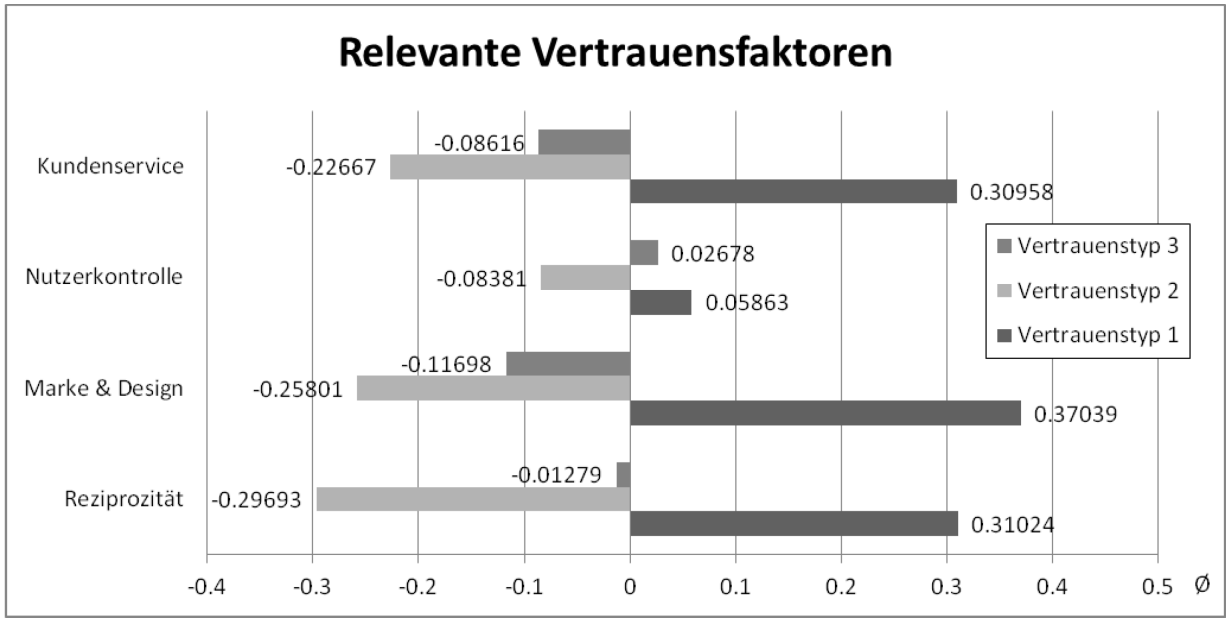


Abbildung 42: Zusammenfassung der relevanten Vertrauensfaktoren pro Vertrauenstyp (Interpretation: negative Werte tendieren zu „trifft zu", positive Werte zu „trifft nicht zu")

Es wurde gezeigt, dass Internetnutzer aufgrund ihres Vorschussvertrauens unterschiedlich in eine Situation einsteigen und bestimmte Vertrauenstypen während einer Transaktion auf unterschiedliche Vertrauensfaktoren achten. Doch können auch Aussagen getroffen werden, ob diese Vertrauenstypen eine Transaktion unterschiedlich abschliessen? Können Aussagen über das Vertrauen als Resultat gemacht werden? Diesen Fragen geht das nächste Kapitel nach.

3.2.3 Vertrauensabsicht pro Vertrauenstyp

In diesem Kapitel wird untersucht, inwiefern Vertrauen als Resultat vorangegangener Transaktionen betrachtet werden kann. Ist eine erneute Transaktion wahrscheinlich? Unterscheiden sich die zukünftigen Verhaltensweisen pro Vertrauenstyp? Die letzte Forschungsfrage widmet sich genau dieser Thematik: „Unterscheiden sich die Vertrauenstypen in Bezug auf die Vertrauensabsichten?" Diese Forschungsfrage beschäftigt sich also mit der Ex-post-Betrachtung von Vertrauen.

Anhand des Kruskal-Wallis-Tests wird untersucht, ob sich die Vertrauenstypen anhand des Faktors Vertrauensabsicht unterscheiden (Kruskal & Wallis, 1952; Hirsig, 2001).

	Vertrauensabsicht
Chi-Quadrat	.915
Asymp. Sig.	.633

Tabelle 17: Kruskal-Wallis-Test der Vertrauensabsicht (Kruskal Wallis Test / Grouping Variable: Ward-Method CLU3_1

Die Signifikanz von .633 zeigt deutlich, dass sich die drei Vertrauenstypen nicht anhand des Faktors Vertrauensabsicht unterscheiden lassen (Tabelle 17). Der Faktor Vertrauensabsicht ist somit für alle drei Vertrauenstypen ähnlich relevant.

Der Mittelwertvergleich des Faktors Vertrauensabsicht in Tabelle 18 unterstützt die Aussage des Kruskal-Wallis-Tests und zeigt, dass sich auch die Mittelwerte nur minimal im Bereich von +/- 0.0 unterscheiden.

Ward Methode	Mittelwert Vertrauensabsicht	Standardabweichung
Typ 1 (n = 524)	.0805957	1.26931307
Typ 2 (n = 526)	-.0484374	.74633824
Typ 3 (n = 499)	-.0335754	.90483898
Total (n = 1'549)	.0000000	1.00000000

Tabelle 18: Mittelwertvergleich des Faktors Vertrauensabsicht pro Vertrauenstyp (Interpretation: negative Werte tendieren zu „trifft zu", positive Werte zu „trifft nicht zu")

Bei der Interpretation der Mittelwerte des Faktors Vertrauensabsicht ist zu erwähnen, dass negative Abweichungen eine Tendenz in Richtung „trifft zu" und positive Werte eine Tendenz in Richtung „trifft nicht zu" andeuten. Der Mittelwert des Faktors Vertrauensabsicht liegt beim Vertrauenstyp 1 im positiven Bereich (Ø .081), was auf eine im Vergleich weniger positive Einschätzung des zukünftigen Vertrauens hindeutet. Vertrauenstyp 2 und 3 jedoch liegen im negativen Bereich (Ø -.048 und Ø -.034) und deuten somit auf positive zukünftige Vertrauenshandlungen hin. Alle 3 Vertrauenstypen geben an, eine hohe Vertrauensabsicht zu haben. Aufgrund der fehlenden Signifikanz kann der Faktor Vertrauensabsicht jedoch nicht als Vergleichskriterium herangezogen werden.

Im Anhang 7.7.1 ist im Detail ersichtlich, wie die drei Vertrauenstypen die Items des Faktors Vertrauensabsicht bewertet haben. Im Ergebniskapitel 4.3 werden mögliche Beweggründe diskutiert, weshalb alle drei Vertrauenstypen zu einer hohen Vertrauensabsicht tendieren könnten. Im folgenden Kapitel 3.2.4 werden die Erkenntnisse der Hauptuntersuchung nochmals übersichtlich zusammengestellt.

3.2.4 Zusammenfassung der Hauptuntersuchung

Anhand der drei Merkmalsvariablen Vertrauen in den Anbieter, Vertrauensneigung und Vertrauen in die Institution wurden durch die Clusteranalyse drei verschiedene Vertrauenstypen identifiziert. Mittels Diskriminanzanalyse konnte bestätigt werden, dass sich alle drei Merkmalsvariablen zur Unterscheidung der Cluster eignen und aufgrund ihrer signifikanten Trennkraft für die Analyse der drei Vertrauenstypen verwendet werden können. Die Ergebnisse der Cluster Analyse können aufgrund der Güteprüfung durch die Diskriminanzanalyse als sehr gut bewertet werden.

Mithilfe eines Mittelwertvergleichs wurden die relevanten Vertrauensfaktoren pro Vertrauenstyp identifiziert. Der Vertrauenstyp 1 achtet im Vergleich am wenigsten auf die Vertrauensfaktoren. Vertrauenstyp 2 achtet auf alle vier Vertrauensfaktoren: das Reziprozitätsverhältnis, die Marke und das Design, den Kundenservice sowie die Nutzerkontrolle. Vertrauenstyp 3 achtet insbesondere auf die Marke und das Design, auf den Kundenservice eines Online-Geschäftsmodell-Anbieters sowie auf das Reziprozitätsverhältnis, wie in Abbildung 43 dargestellt ist.

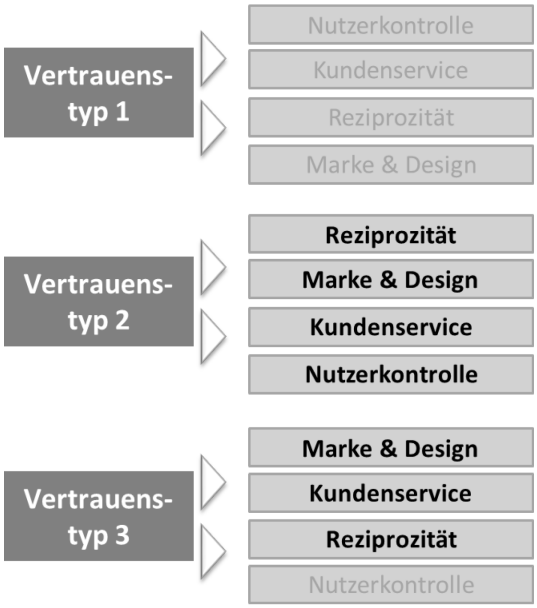


Abbildung 43: Zusammenfassung der forschungsmethodischen Ergebnisse (eigene Darstellung)

Wiederum mithilfe eines Mittelwertvergleichs wurde untersucht, inwiefern sich die drei Vertrauenstypen in Bezug auf ihre Vertrauensabsichten unterscheiden. Der Kruskal-Wallis-Test ergab jedoch, dass der Faktor Vertrauensabsicht für die Unter-

scheidung der drei Vertrauenstypen nicht signifikant ist und deshalb nicht als Unterscheidungskriterium herangezogen werden kann.

Im nächsten Kapitel 4 „Diskussion der Ergebnisse“ werden die Erkenntnisse dieses Methodenkapitels im Detail analysiert und interpretiert.

4 Diskussion der Ergebnisse

Dieses Kapitel widmet sich der ausführlichen Analyse und Interpretation der Ergebnisse des Methodenkapitels. Im ersten Kapitel 4.1 werden die drei identifizierten Vertrauenstypen detailliert interpretiert und anschliessend benannt. Im Kapitel 4.2 werden die identifizierten relevanten Vertrauensfaktoren pro Vertrauenstyp im Einzelnen erörtert. Danach werden im Kapitel 4.3 die Vertrauensabsichten der Vertrauenstypen diskutiert und zuletzt werden die Ergebnisse der drei Forschungsfragen im Kapitel 4.4 zusammengefasst. Abbildung 44 stellt den Aufbau dieses Kapitels nochmals grafisch dar und liefert einen Überblick über die drei zu beantwortenden Forschungsfragen.

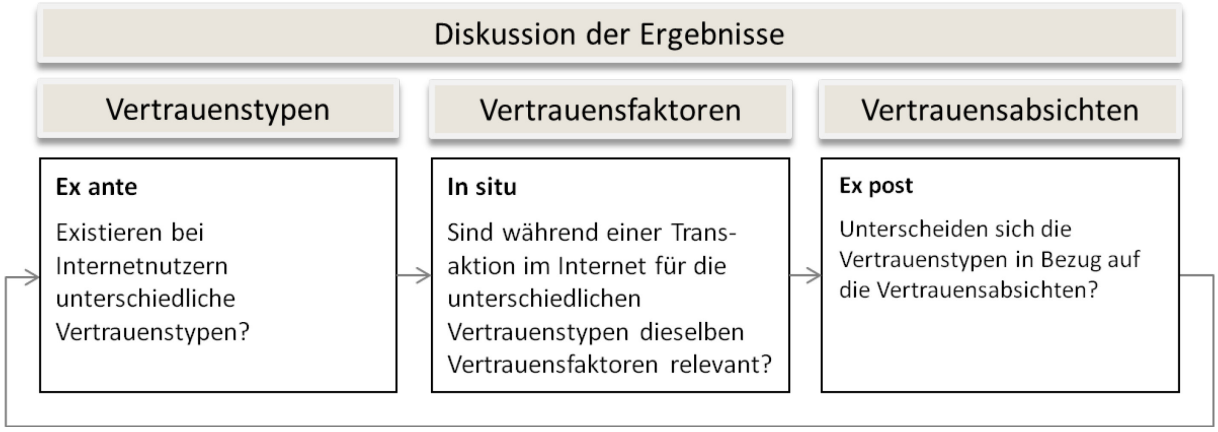


*Abbildung 44: Übersicht über das Kapitel 4 „**Diskussion der Ergebnisse**“ (eigene Darstellung)*

Für die Diskussion der Ergebnisse soll nochmals darauf hingewiesen werden, dass Mittelwerte eines Faktors als -1 „trifft zu“ und +1 „trifft nicht zu“ interpretiert werden. Die Mittelwerte der einzelnen Items der Faktoren hingegen werden als 1 „trifft zu“ und 5 „trifft nicht zu“ interpretiert. Ausserdem soll erwähnt werden, dass in diesem Ergebniskapitel ein Perspektivenwechsel von der rein wirtschaftswissenschaftli-

chen Interpretation der Ergebnisse zu einer praxisorientierten Sichtweise stattfindet. Da die drei Vertrauenstypen modellartig beschrieben und charakterisiert werden, führt dies auch automatisch zu einer reduktionistischen Sichtweise. Dies ermöglicht es, pauschalisierte Aussagen für Anbieter von Online-Geschäftsmodellen über die drei Vertrauenstypen zu machen.

4.1 Jeder vertraut anders: Interpretation der drei Vertrauenstypen

Um die erste Forschungsfrage „Existieren bei Internetnutzern unterschiedliche Vertrauenstypen?“ beantworten zu können, wurden im Kapitel 3.2.1 mittels Clusteranalyse drei verschiedene Vertrauenstypen identifiziert. Die Ergebnisse werden nun in diesem Kapitel detailliert betrachtet und analysiert. In den Kapiteln 4.1.1 bis 4.1.3 werden die drei Vertrauenstypen anhand der für die Clusterung verwendeten Faktoren Vertrauen in den Anbieter, Vertrauensneigung, Vertrauen in die Institution sowie anhand demografischer Faktoren und Internetnutzung analysiert. Im Kapitel 4.1.4 werden die drei Vertrauenstypen einander gegenübergestellt und benannt.

4.1.1 Interpretation Vertrauenstyp 1

Dieses Kapitel widmet sich der detaillierten Analyse und Beschreibung des Vertrauenstyps 1. Zuerst wird die Interpretation aufgrund der Faktoren der Clusterung vorgenommen, um danach den Vertrauenstyp anhand demografischer Unterscheidungsmerkmale sowie der Internetnutzung zu charakterisieren.

4.1.1.1 Interpretation Vertrauenstyp 1 aufgrund der Clusterung

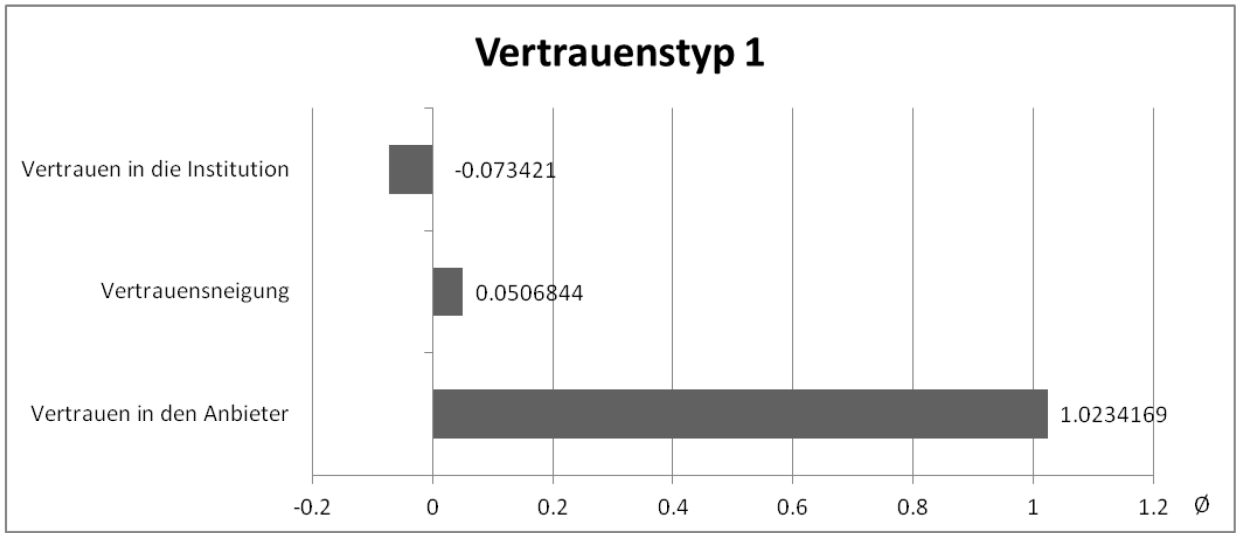


Abbildung 45: Analyse Vertrauenstyp 1 anhand des Mittelwertes Ø (Interpretation: negative Werte tendieren zu „trifft zu", positive Werte zu „trifft nicht zu")

Vertrauen in den Anbieter: Betrachten wir zuerst den Faktor Vertrauen in den Anbieter. Im Kapitel 3.2.1 haben wir anhand der Tabelle 11 (Prüfung der Merkmalsvariablen, S. 134) festgestellt, dass der Faktor Vertrauen in den Anbieter besonders gut für die Trennung der Cluster geeignet ist. Deshalb steht dieser Faktor im Folgenden auch im besonderen Fokus der Analyse. Wie aus Abbildung 45 hervorgeht, hebt sich Typ 1 ganz klar durch sein vergleichsweise niedriges Vertrauen in den Anbieter ab (Ø 1.02). Im Anhang 7.5.4 sind die detaillierten Auswertungen der Items pro Vertrauenstyp aufgeführt. Vertrauenstyp 1 schätzt seinen Anbieter weder als wohlwollend (71.8 % „neutral" bis „trifft nicht zu") noch als kompetent (57.4 % „neutral" bis „trifft nicht zu"), ehrlich (75.6 % „neutral" bis „trifft nicht zu"), zuverlässig (65.7 % „neutral" bis „trifft nicht zu"), vertrauenswürdig (72.9 % „neutral" bis „trifft nicht zu") oder sympathisch ein (66.2 % „neutral" bis „trifft nicht zu"). Auch überlässt er ihm ungern persönliche Daten (71.5 % „neutral" bis „trifft nicht zu") und verlässt sich nicht auf die Angebotsqualität (58.2 % „neutral" bis „trifft nicht zu"). Vertrau-

enstyp 1 hat im Vergleich zu den anderen Typen ein niedriges Vertrauen in den Anbieter.

Aufgrund des niedrigen Vertrauens in den Anbieter ist davon auszugehen, dass für Vertrauenstyp 1 bei der Auswahl des Anbieters andere Beweggründe als Vertrauen im Vordergrund gestanden haben. Zum Beispiel könnte es sein, dass er die Transaktion mit dem Anbieter aufgrund des niedrigen Preises, der Zeitersparnis, der Ortsunabhängigkeit oder dem Bedürfnis nach sozialem Austausch durchgeführt hat. Vertrauenstyp 1 scheint ein sehr selektiver Mensch zu sein, der bei Weitem nicht jedem Anbieter im Netz traut. In der Folge wird dieser Vertrauenstyp anhand der weiteren Auswertungen näher beschrieben.

Vertrauensneigung: Der Faktor Vertrauensneigung beinhaltet die eigene Einschätzung der Bereitschaft, anderen Menschen im realen Leben zu vertrauen (McKnight et al., 2002a) und ist eine Eigenschaft des Vertrauensgebers (Mayer et al., 1995). Das Verhalten der Menschen in der realen Welt, ihre Bedürfnisse und Vorlieben beeinflussen auch wesentlich ihr Verhalten im Online-Umfeld (Renner, Schütz & Machilek, 2005). Der Vertrauenstyp 1 hat eine vergleichsweise neutrale, leicht positive Vertrauensneigung (Ø 0.05) (Abbildung 45), was darauf hindeutet, dass dieser Vertrauenstyp anderen Menschen gegenüber eine neutrale bis eher negative Vertrauensbereitschaft aufbringt. Im Anhang 7.5.5 sind die detaillierten Auswertungen des Faktors Vertrauensneigung für Vertrauenstyp 1 aufgeführt. Typ 1 hat zwar grundsätzlich Vertrauen zu anderen Menschen (53.4 % „trifft zu“ oder „trifft eher zu“), dafür verlässt er sich im konkreten Fall nicht auf andere Menschen (36.5 % „trifft eher nicht zu“ oder „trifft nicht zu“). Er hat zwar Vertrauen in die Menschheit (35.7 % „trifft zu“ oder „trifft eher zu“), findet aber nicht, dass Menschen generell zuverlässig sind (33.9 % „trifft eher nicht zu“ oder „trifft nicht zu“). Diese Ambivalenz bewirkt, dass sich die Vertrauensneigung des Typs 1 eher im neutralen Bereich befindet.

Es scheint, dass Vertrauenstyp 1 überzeugt ist, dass er sich auf andere verlassen kann, es aber im konkreten Fall doch nicht macht. Dieses ambivalente Verhalten könnte darauf hindeuten, dass ihm das Bauchgefühl sagt, dass er anderen Menschen und der Menschheit vertrauen kann, sein Verstand es aber nicht zulässt, dass er sich auch auf diese verlässt. Um sich auf andere verlassen zu können, muss man bereit sein, loszulassen und einen Teil der Kontrolle abzugeben. Das damit verbundene Risiko möchte dieser Vertrauenstyp lieber nicht eingehen. Sich auf andere zu verlassen heisst, Verantwortung abzugeben und zu delegieren. Eventuell hat Vertrauens-

typ 1 Angst, enttäuscht zu werden, und geht deshalb kein Risiko ein. Dies könnte darauf hindeuten, dass Vertrauenstyp 1 eher ein Individualist und Einzelkämpfer ist. Selbstbestimmung und Kontrolle scheinen für Vertrauenstyp 1 zentral zu sein.

Vertrauen in die Institution: Menschen können gegenüber einer Institution wie dem Medium Internet im Allgemeinen entweder positiv oder negativ eingestellt sein. Wie aus Abbildung 45 hervorgeht, vertraut Typ 1 dem Medium Internet tendenziell, aber nur sehr mässig (Ø -0.07).

Im Anhang 7.5.6 sind die detaillierten Auswertungen des Faktors Vertrauen in die Institution für Vertrauenstyp 1 aufgeführt. Die Frage, ob Online-Anbieter ihre Kunden grundsätzlich anständig behandeln, beantwortet Typ 1 neutral (51.9 % „neutral“). Er findet jedoch, dass ihn Sicherheitsmechanismen (31.9 % „trifft zu“ oder „trifft eher zu“), rechtliche Rahmenbedingungen (34.0 % „trifft zu“ oder „trifft eher zu“) sowie technische Anwendungen (43.7 % „trifft zu“ oder „trifft eher zu“) vor Problemen im Internet bewahren können und dass das Internet im Allgemeinen eine stabile und sichere Umgebung ist (36.4 % „trifft zu“ oder „trifft eher zu“).

Vertrauenstyp 1 ist im Vergleich kein Internet-Euphoriker, fasst aber doch Vertrauen in die Institution Internet und glaubt an die Möglichkeiten der Technik. Interessant ist, dass dieser Vertrauenstyp dem gewählten Anbieter ganz klar kein Vertrauen entgegenbringt, im Vergleich auch kein Vertrauen in die Menschheit hat, dem Internet als Ganzes gegenüber aber doch tendenziell positiv eingestellt ist. Er vertraut demnach den Sicherheitsmechanismen und den Rahmenbedingungen, nicht aber den Unternehmen und Personen, welche dahinterstehen. Es könnte sein, dass ihm wichtig ist, dass das Internet durch klar geregelte Prozesse der technischen Anwendungen und durch nationale und internationale Gesetze gesichert ist und diese durch eine Vielzahl von Personen und Institutionen kontrolliert werden. Diese Kontrollmechanismen geben ihm ein Mindestmass an Sicherheit, was bei Einzelpersonen und Anbietern nicht der Fall ist. Es scheint, dass Typ 1 auf die Weisheit und die Kontrolle der Vielen vertraut.

Das mässige bis neutrale institutionsbasierte Vertrauen könnte aber auch darauf zurückzuführen sein, dass sich Vertrauenstyp 1 wenige Gedanken über das System Internet gemacht hat oder er das System nicht versteht und deshalb die Fragen eher im neutralen Bereich bewertet hat. Deshalb ist es spannend zu sehen, wie Typ 1 seine Internetnutzung und seine Internetkompetenzen einstuft, was im nächsten Kapitel betrachtet wird.

4.1.1.2 Interpretation Vertrauenstyp 1 anhand demografischer Unterscheidungsmerkmale sowie der Internetnutzung

Die drei Vertrauenstypen unterscheiden sich nicht nur signifikant anhand der für die Clusterung herangezogenen drei Faktoren (Vertrauen in den Anbieter, Vertrauensneigung sowie Vertrauen in die Institution), sondern sie unterscheiden sich durch Alter, höchsten Bildungsabschluss, durch das gewählte Online-Geschäftsmodell, die Nutzung sozialer Netzwerke und Online-Games sowie durch die Wahrnehmung der Sensibilität ihrer Daten signifikant voneinander. Diese Merkmale sind daher besonders gut geeignet, um die Vertrauenstypen zu unterscheiden und zu charakterisieren. Die Signifikanzen sind in Tabelle 19 aufgeführt[43].

		Ward Method
Ward Method	Pearson Correlation	1
	Sig. (2-tailed)	
Geschlecht (V_135)	Pearson Correlation	-.035
	Sig. (2-tailed)	.163
Alter (V_136)	Pearson Correlation	.049
	Sig. (2-tailed)	**.055**
Höchster Bildungsabschluss (V_139)	Pearson Correlation	-.054
	Sig. (2-tailed)	**.033**
Erwerbstätigkeit (V_137)	Pearson Correlation	-.024
	Sig. (2-tailed)	.343
Branchen (V_138)	Pearson Correlation	-.031
	Sig. (2-tailed)	.226
Internetnutzung (V_1)	Pearson Correlation	.026
	Sig. (2-tailed)	.303
Internetnutzung in Jahren (V_2)	Pearson Correlation	.021
	Sig. (2-tailed)	.413
Private oder berufliche Internetnutzung (V_3)	Pearson Correlation	.031
	Sig. (2-tailed)	.220
Gewähltes Online-Geschäftsmodell (V_177)	Pearson Correlation	-.155
	Sig. (2-tailed)	**.000**
E-Mail-Nutzung (V_4)	Pearson Correlation	.041
	Sig. (2-tailed)	.104
Informationssuche (z. B. auf Google) (V_5)	Pearson Correlation	026
	Sig. (2-tailed)	.300
Nutzung von Online-Banking (V_6)	Pearson Correlation	-.005
	Sig. (2-tailed)	.833
Nutzung von sozialen Netzwerken/Online-Communitys (V_7)	Pearson Correlation	.080
	Sig. (2-tailed)	**.002**
Nutzung von Online-Shopping (V_8)	Pearson Correlation	-.033
	Sig. (2-tailed)	.196
Nutzung von Online-Zeitungen (V_1v6)	Pearson Correlation	.028
	Sig. (2-tailed)	.266
Nutzung von Online-TV/-Radio (V_9)	Pearson Correlation	-.005

[43] Es wurde die Korrelation zwischen den Items und den Vertrauenstypen gerechnet.

	Sig. (2-tailed)	.856
Nutzung von Online-Dating (V_10)	Pearson Correlation	.022
	Sig. (2-tailed)	.393
Nutzung von Blogs (V_11)	Pearson Correlation	.025
	Sig. (2-tailed)	.320
Nutzung von Twitter (V_12)	Pearson Correlation	.031
	Sig. (2-tailed)	.226
Nutzung von Online-Games (V_13)	Pearson Correlation	.053
	Sig. (2-tailed)	**.037**
Datensensibilität	Pearson Correlation	-.319
	Sig. (2-tailed)	**.000**

Tabelle 19: Signifikanzen der Demografie und der Internetnutzung

Tabelle 19 beinhaltet weitere, jedoch nicht signifikante Unterscheidungsmerkmale der drei Cluster. Renner et al. (2005) betonen, dass finanzielle, bildungs- und ortsbezogene, aber auch kulturelle und situative Bedingungen für das Verhalten im Internet relevant sind. Weiter weisen sie darauf hin, dass die bisherige „Internetkarriere" von entscheidender Bedeutung für den Umgang mit dem Internet ist. Beaudoin (2008) konnte aufzeigen, dass die Internetnutzung einen direkten Einfluss auf das Vertrauen im Internet hat. Ebenso weisen Lee und Turban (2001) darauf hin, dass Menschen, welche unsicher im Netz sind und die Prozesse des Internets nicht verstehen, dem Internet und seinen Anbietern weniger Vertrauen entgegenbringen (ebenso Shankar, Urban & Sultan, 2002). Einige Forscher konnten aufzeigen, dass Geschlechtsunterschiede den Umfang und Art der Internetnutzung und somit der Wahrnehmung von Vertrauenswürdigkeit im Netz beeinflussen (Venkatesh & Morris, 2000; Sheehan, 1999; Renner et al., 2005). Deshalb werden in diesem Kapitel neben den soziodemografischen Faktoren auch die Internetnutzung und die Internetkompetenz der drei Vertrauenstypen ausgewertet und analysiert, was zu einem tieferen Verständnis der Typen beitragen soll. Im Folgenden werden die drei Vertrauenstypen zuerst anhand der signifikanten, danach anhand der nicht signifikanten Faktoren ausgewertet.

Signifikante Unterscheidungsmerkmale

Alter: In Abbildung 46 wird deutlich, dass der Vertrauenstyp 1 relativ jung ist, grösstenteils aus unter 25-Jährigen (26.2 %) sowie 26- bis 45-Jährigen (27.7 %) besteht (siehe auch Anhang 7.5.7). Bei Vertrauenstyp 1 scheint es sich demnach vorwiegend um Digital Natives zu handeln, welche von klein auf mit der Technologie des neuen Internets aufgewachsen sind (Prensky, 2001; Palfrey & Gasser, 2008). Deshalb wird

diese Altersgruppe ab Jahrgang 1980 (Palfrey & Gasser, 2008) auch oft als Generation Internet bezeichnet. Zum Zeitpunkt der Umfrage im Dezember 2010 und Januar 2011 zählen demnach die 31-Jährigen noch zu den Digital Natives. Daraus könnte man schliessen, dass dieser Typ vergleichsweise hohes Vertrauen in die Institution Internet hat. Ziehen wir für diese Annahme den Faktor Vertrauen in die Institution von Vertrauenstyp 1 (Abbildung 39) heran, wird ersichtlich, dass Typ 1 dem Medium Internet zwar tendenziell vertraut, jedoch nur mässig. Es scheint, dass dieser Vertrauenstyp mit dem Umgang im Netz vertraut ist, jedoch das Medium Internet auch kritisch betrachtet und hinterfragt. Der Digital Native kann sich ein Leben ohne Internet gar nicht vorstellen und sein Leben lässt sich nicht strikt in Online- und Offline-Domäne unterscheiden. Er weiss, dass es im Leben nichts um sonst gibt und dass es zum Wesen des Internets gehört, dass er bei der Nutzung ebenfalls benutzt wird.

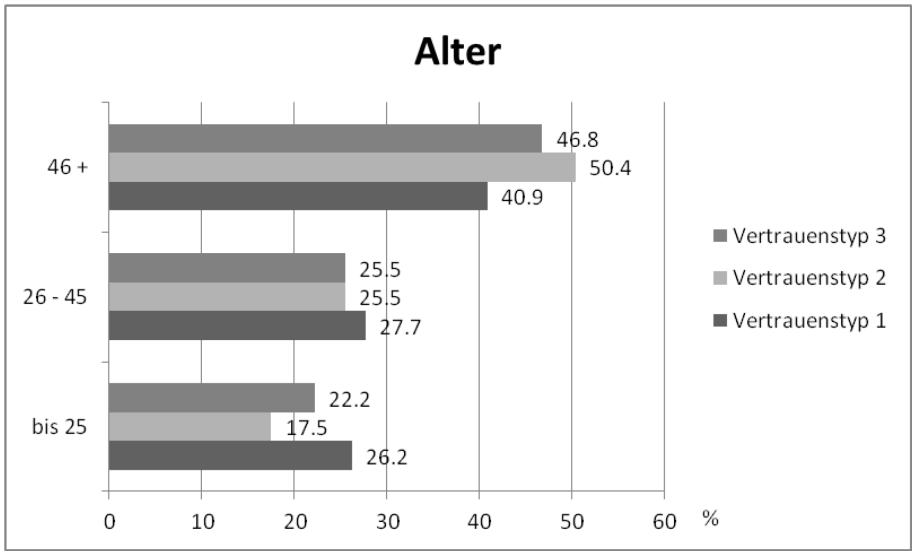


Abbildung 46: Typenunterscheidung anhand des Alters in Prozent (V_136)

Bildung: Vertrauenstyp 1 ist vergleichsweise sehr gut gebildet oder noch immer in Ausbildung. Knapp ein Drittel der Vertrauenstyp 1 zugehörigen Nutzer verfügen über einen höheren Bildungsabschluss, 28.4 % haben ein Fachhochschul- oder Universitätsstudium abgeschlossen (Anhang 7.5.7). Da es sich beim Vertrauenstyp 1 um das jüngste Cluster handelt, ergibt es Sinn, dass sich ein Grossteil der Probanden (15.3 %) noch in Ausbildung befindet. Es könnte die Annahme getroffen werden, dass die Probanden das Internet mit steigendem Bildungsgrad häufiger nutzen. Dies wird wiederum weiter unten bei der Internetnutzung verglichen. Dieser Vertrauenstyp scheint sehr kopflastig zu sein, man könnte sogar die Vermutung wagen, dass er

emotional eher ein unsicherer Typ ist. Die bisherigen Auswertungen haben gezeigt, dass dieser Typ eher dem Internet als Institution statt den Menschen und Anbietern selbst vertraut. Er verbringt sehr viel Zeit alleine über seinen Büchern und hat eventuell wenig direkten Kontakt zu seinen Mitmenschen und deshalb auch eher eine geringe Vertrauensneigung.

Weiter könnte die Vermutung aufgestellt werden, dass es sich bei diesem Vertrauenstyp um eine Personengruppe handelt, die gerne auf einen Plan B zurückgreift. Die mässige Vertrauensneigung und das tiefe Vertrauen in den Anbieter gibt Hinweise darauf, dass er sich mit einer Exit-Strategie wohlfühlt. Verbindlichkeit und Kontinuität sind vermutlich keine Eigenschaften dieses Vertrauenstyps. Aus mehreren Optionen die geeignete zu wählen, könnte das tiefe Vertrauen in den Anbieter und die Menschen etwas abfedern. Ausserdem hat er so das Gefühl, immer die Kontrolle über sein Leben zu haben. Virtuelle Identitäten können konstruiert und bei negativer Resonanz sofort wieder gelöscht werden.

Gewähltes Online-Geschäftsmodell und konkreter Anbieter: In der Umfrage wurden die Probanden nach dem konkreten Geschäftsmodell gefragt, bei welchem sie sich als Letztes angemeldet haben: „Denken Sie an den letzten Online-Anbieter, bei dem Sie sich als Nutzer registriert haben, wobei die Anmeldung die Eingabe einiger persönlicher Daten erforderte (z. B. für das Anlegen eines persönlichen Nutzer-Profils). Um welche Art von Online-Angebot handelte es sich dabei?“ Es wird angenommen, dass das von den Teilnehmern gewählte Online-Geschäftsmodell einen starken Einfluss auf die Beantwortung der Fragen hatte, insbesondere zum Beispiel auf die Einschätzung der Vertrauenswürdigkeit des Anbieters. Die Beweggründe, einen Anbieter aufzusuchen, unterscheiden sich pro Geschäftsmodell stark, ebenso profitieren einige Geschäftsmodelle von einem positiven Image, während andere an einem eher negativen Ruf leiden.

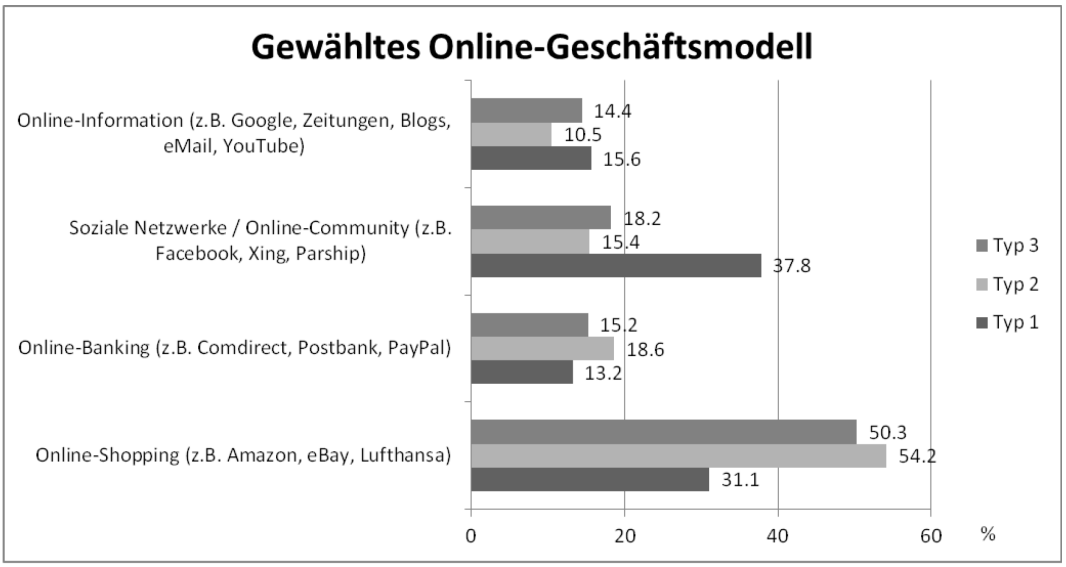


Abbildung 47: Typenunterscheidung anhand des gewählten Online-Geschäftsmodells in Prozent (V_177)

Wie in Abbildung 47 ersichtlich, hat sich Vertrauenstyp 1 im Vergleich am häufigsten als Nutzer eines sozialen Netzwerkes/einer Online-Community (37.8 %) oder bei einem Online-Informationen-Anbieter (15.6 %) angemeldet (Anhang 7.5.9). Beim Online-Banking (13.2 %) und beim Online-Shopping (31.1 %) jedoch liegt er hinter den beiden anderen Vertrauenstypen. Es interessiert nun, bei welchen konkreten Anbietern sich Vertrauenstyp 1 genau angemeldet hat. Da bei der Befragung nach dem konkreten Anbieter ein Textfeld programmiert und keine Bewertung abgefragt wurde, kann zum konkreten Anbieter keine Korrelation und Signifikanz berechnet werden. Da diese Frage sehr eng an das gewählte Geschäftsmodell gekoppelt ist, wird die Auswertung trotzdem an dieser Stelle besprochen. Die typenvergleichende Grafik ist im Anhang 7.5.9 unter Abbildung 96 einsehbar. Dabei ist besonders auffallend, dass Vertrauenstyp 1 sich mit Abstand am meisten neu bei Facebook registriert hat (23.7 % im Vergleich zu 6.1 % Typ 2 und 4.6 % Typ 3). Bei den Online-Informationen sticht Vertrauenstyp 1 durch seine Anmeldungen bei Google (3.8 %) sowie bei YouTube (1.7 %) hervor.

Soziale Netzwerke und Online-Communitys verlangen aufgrund des Geschäftsmodells viele persönliche und aktuelle Informationen, welche den Nutzer oft identifizierbar und somit verletzlich machen (Nosko et al., 2010). Vertrauenstyp 1 ist durch sein im Vergleich niedriges Vertrauen in den Anbieter aufgefallen. Es könnte sein, dass bei dem gut gebildeten Typ 1 die vielen kritischen Pressemeldungen der vergangen Jahre über soziale Netzwerke, insbesondere über die Handhabung des Da-

tenschutzes bei Facebook, einen negativen Eindruck hinterlassen haben. Weiter haben sich Vertreter des Vertrauenstyps 1 vergleichsweise oft bei Google neu registriert. Auch Google wurde in Bezug auf die Datensammelwut medial thematisiert und als Datenkrake bezeichnet. Es könnte demnach sein, dass das gewählte Online-Geschäftsmodell den Faktor Vertrauen in den Anbieter mitbeeinflusst hat. Es scheint, dass sich Vertrauenstyp 1 gerne über Google und YouTube informiert, und es könnte sein, dass er durch Fachgespräche bereits über viele Informationen über unterschiedliche Anbieter verfügt, noch bevor er sich für einen Anbieter entscheidet. Es scheint, dass bei der Nutzung von Online-Diensten für ihn das Ziel im Vordergrund steht und er möglichst schnell zu einem guten Resultat kommen möchte.

Diese Auswertung hat gezeigt, dass sich Vertrauenstyp 1 überdurchschnittlich oft bei sozialen Netzwerken und Online-Information-Anbieter neu registriert hat. Interessant ist nun, ob Vertrauenstyp 1 diese Geschäftsmodelle auch oft nutzt.

Nutzung von Online-Diensten (soziale Netzwerke & Online-Games): Man ist versucht zu denken, dass insbesondere jüngere Menschen überdurchschnittlich oft soziale Netzwerke und Online-Games nutzen. Betrachten wir die Daten im Anhang 7.5.7, zeigt sich, dass Typ 1 mit 52.5 % täglicher oder mehrmaliger Nutzung pro Woche effektiv Spitzenreiter bei sozialen Netzwerken und Online-Communitys ist. Vertrauenstyp 1 ist demnach ein häufiger Nutzer von sozialen Netzwerken. Dies könnte dahingehend interpretiert werden, dass für Nutzer dieses Typs das soziale Umfeld sehr wichtig ist und, da es sich grösstenteils um Digital Natives handelt, auch das engere Umfeld im Umgang mit den Sozialen Medien geübt ist. So pflegt Vertrauenstyp 1 seine Beziehungen ganz selbstverständlich über das Internet.

Es wurde aber auch erwogen, dass Vertrauenstyp 1 eher kopflastig ist und eventuell unter Selbstwertproblemen leiden könnte. Nun könnte die Annahme getroffen werden, dass er in seinen Sozialkompetenzen im Alltag zu wenig geübt ist und deshalb seine Kontakte lieber im Internet pflegt, was das gewählte Geschäftsmodell und die häufige Nutzung von sozialen Netzwerken erklären könnte. Die technische Barriere könnte ihm als emotionalen Schutzwall dienen, welcher Mimik und Gestik ausblendet. Im Internet könnte ihm seine konstruierte Identität Selbstsicherheit verleihen. Ihm ist Kontrolle und Souveränität wichtig und bei virtuellen sozialen Beziehungen kann er sich für Antworten genügend Bedenkzeit nehmen oder sich einer Konversation durch Log-out entziehen. Vertrauenstyp 1 hat vermutlich das Gefühl, dass er im Netz seine sozialen Beziehungen im Griff hat.

Bei der Nutzung von Online-Games liegt Vertrauenstyp 1 im Mittelfeld (23.5 % „jeden Tag“ bis „mehrmals pro Woche“, Anhang 7.5.7). Es könnte sein, dass insbesondere bei den Online-Games das Bildungsniveau eine gewichtige Rolle spielt, welches bei Vertrauenstyp 1 besonders hoch ist. Diese Annahme wird bei den anderen beiden Vertrauenstypen wieder aufgenommen.

Datensensibilität: Bei der Frage „Ich finde es unproblematisch, dem gewählten Anbieter persönliche Daten zu überlassen.“ antwortet Vertrauenstyp 1 zu 28.2 % mit „trifft eher nicht zu“ oder mit „trifft nicht zu“ (zum Vergleich: Vertrauenstyp 2 zu 4.0 % und Vertrauenstyp 3 zu 11.0 %) (siehe Anhang 7.5.4). Er sagt demnach aus, dass er es problematisch findet, dem Anbieter persönliche Daten zu überlassen, ist also eher restriktiv eingestellt, was die Verbreitung seiner persönlichen Daten angeht. Beim Ausfüllen dieser Umfrage jedoch hat Vertrauenstyp 1 bei den Fragen zur Demografie und der Internetnutzung am wenigsten „Keine Antwort“ angekreuzt, wie in Anhang 7.5.10 abzulesen ist (Typ 1 hat bei neun von 18 Fragen am wenigsten keine Antwort angegeben). Oder anders formuliert: Vertrauenstyp 1 hat am häufigsten alle Fragen beantwortet und somit freiwillig Angaben über die eigene Person gemacht. Des Weiteren nutzt Typ 1 überdurchschnittlich oft soziale Netzwerke und Online-Communitys, bei welchen viele persönliche Daten zur Verfügung gestellt werden müssen (Nosko et al., 2010). Diese Diskrepanz zwischen der Aussage und dem Verhalten kann mit dem Privacy-Paradox erklärt werden (Theoriekapitel 2.2.2.2), welches besagt, dass trotz Privacybedenken private Daten im Internet offengelegt werden, wenn der wahrgenommene Nutzen der Preisgabe höher ist als die eingegangenen Risiken (Barnes, 2006; Norberg et al., 2007; Acquisti & Gross, 2007). Ausserdem wurde bei der Auswertung zum Alter bereits diskutiert, dass dem Digital Native bewusst sein könnte, dass der Datenaustausch ganz selbstverständlich zum Internet mit dazugehört.

Nicht signifikante Unterscheidungsmerkmale

Geschlecht: Vertrauenstyp 1 ist zu 47.1 % weiblich und zu 50.6 % männlich (2.3 % haben nichts angekreuzt). Wird die Zusammensetzung der Gesamtstichprobe dieser Umfrage oder auch die Grundgesamtheit in Deutschland betrachtet, fällt auf, dass jeweils die Frauen untervertreten sind (Grundgesamtheit Deutschland 2009: 51 % weiblich) (Destatis, 2010b). Dass die Männer bei diesem Vertrauenstyp stärker vertreten sind, sticht demnach hervor.

Erwerbstätigkeit und Branchen: Ein grosser Anteil des Vertrauenstyps 1 befindet sich noch in Ausbildung (15.3 %), was sich mit dem hohen Anteil an eher jüngeren Personen deckt. Beruflich ist der Typ 1 verstärkt im Gesundheits- und Sozialwesen (7.6 %) tätig (Anhang 7.5.7). Gesundheits- und Sozialwesen sind Branchen, bei denen die Verantwortlichen sehr oft mit Schicksalsschlägen und Notlagen ihrer Kunden in Berührung kommen. Dieser Vertrauenstyp hat in seinem Berufsleben schon vieles erlebt und sein anfänglich positives Menschenbild hat sich seiner Realität angepasst. Dies könnte eine Erklärung für die ambivalente Vertrauensneigung sein. Um nicht selbst am Erlebten zu zerbrechen, muss sich Vertrauenstyp 1 ganz klar abgrenzen können. Sein Bauchgefühl sagt ihm noch immer, dass Menschen vertrauenswürdig sind, seine berufliche Erfahrung jedoch lässt ihn skeptischer werden.

Internetnutzung: Der Vertrauenstyp 1 verfügt über eine geringere Interneterfahrung, die Intensität der Internetnutzung liegt im Mittelfeld. Die Nutzungshistorie liegt im untersten Bereich: 25.1 % nutzen es seit weniger als fünf Jahren, dafür nutzen insgesamt 91.8 % das Internet täglich. Bei der Analyse, ob er das Internet beruflich oder privat nutzt, weist Typ 1 mit 48.6 % die niedrigste private Nutzungsrate auf. Ausschliesslich beruflich nutzt das Internet in dieser Umfrage jedoch fast niemand (Anhang 7.5.7). Insbesondere die geringe Intensität der Internetnutzung erstaunt, da es sich beim Typ 1 um Digital Natives und um gut gebildete oder sich noch in Ausbildung befindende Personen handelt. Eigentlich würde man annehmen, dass genau diese Personen auffallend oft im Internet sind. Es könnte aber sein, dass Personen, welche beruflich am PC arbeiten, die jungen Studenten in der täglichen Nutzung übertreffen.

Bei der Diskussion zum institutionsbasierten Vertrauen wurde hinterfragt, ob die neutrale Beurteilung des Vertrauens ins Internet auf eine geringe Internetkompetenz zurückzuführen seien. Die geringe Interneterfahrung von Vertrauenstyp 1 gibt diesen Überlegungen Aufwind, der Zusammenhang kann jedoch nicht nachgewiesen werden und bleibt deshalb nach wie vor eine Vermutung.

Nutzung von Online-Diensten: Neben den bereits ausgewerteten Online-Diensten soziale Netzwerke und Online-Games bestehen weitere Online-Dienste, welche jedoch keine signifikante Trennkraft der Cluster aufweisen konnten. Typ 1 ist gegenüber dem Online-Banking eher skeptisch, er macht von diesem Dienstleistungsangebot am seltensten gebrauch (42.0 % „jeden Tag“ bis „mehrmals pro Woche“). Typ 1 liest am meisten mehrmals pro Woche seine Zeitung online (35.8 %) und ist auch bei der Nutzung von Twitter Spitzenreiter (7.1 % „jeden Tag“ bis „mehrmals

pro Woche“). Zusammenfassend liegt Vertrauenstyp 1 bei der Nutzung von Online-Diensten im Mittelfeld (drei Spitzenpositionen von möglichen elf) (Anhang 7.5.9).

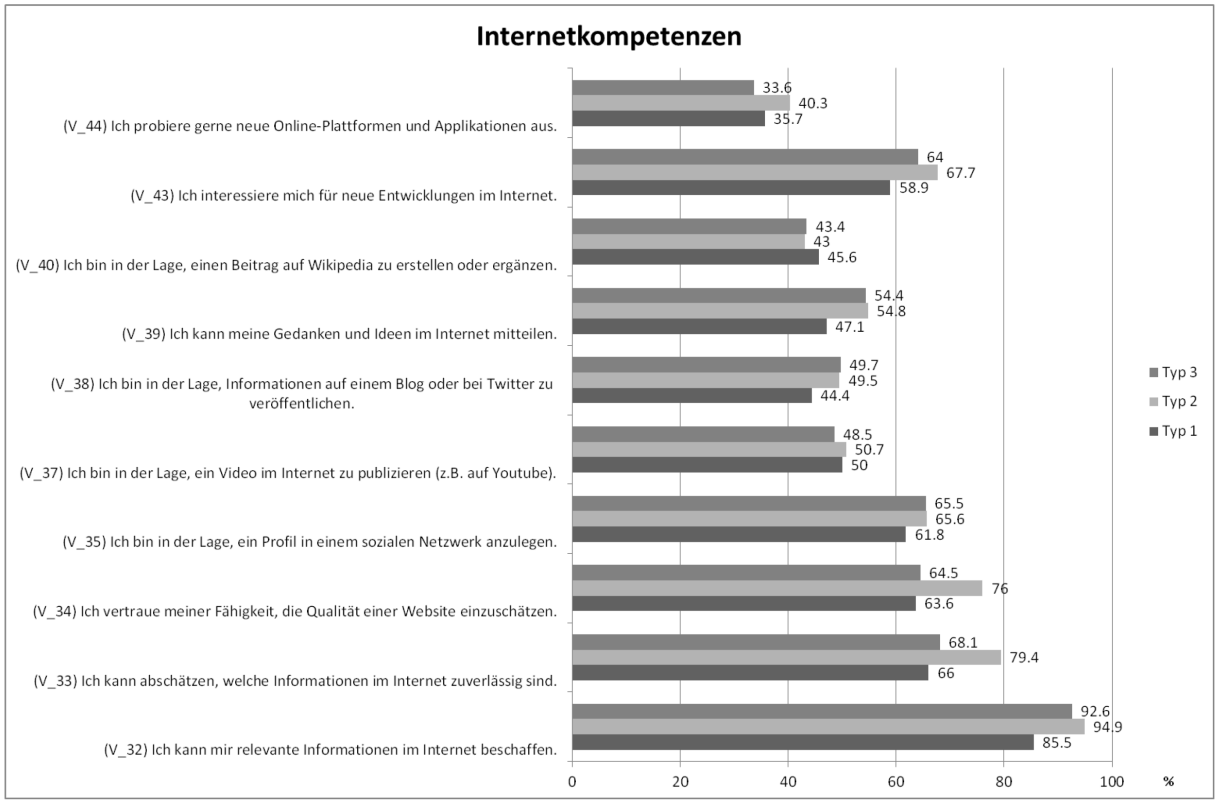


Abbildung 48: Typenunterscheidung anhand der Internetkompetenzen in Prozent bei „trifft zu“ und „trifft eher zu“

Internetkompetenzen: Vertrauenstyp 1 fühlt sich im Vergleich zu den anderen Typen (Abbildung 48 und Anhang 7.5.8) am besten in der Lage, einen Beitrag auf Wikipedia zu erstellen oder zu ergänzen (45.6 % „trifft zu“ und „trifft eher zu“). Ansonsten schätzt er sich selbst als nicht sehr internetaffin ein und er nutzt das Internet im Vergleich zu den anderen Typen erst seit kürzerer Zeit (25.1 % nutzen es seit weniger als fünf Jahren).

Vertrauenstyp 1 schätzt seine Internetkompetenzen im Vergleich zu den anderen beiden Typen am geringsten ein. Dies ist interessant, weil es sich um eine gut gebildete bzw. sich noch in Ausbildung befindenden Personengruppe handelt. Man würde meinen, dass das Studium dazu zwingt, sich relevante Informationen im Internet zu beschaffen und Qualitätsunterschiede von Webseiten schnell zu erkennen, was jedoch bei Vertrauenstyp 1 nicht der Fall zu sein scheint. Es könnte jedoch sein, dass Vertrauenstyp 1 enorm hohe Ansprüche an sich stellt. Die Auswertungen haben gezeigt, dass er die meisten Internetdienste regelmässig nutzt. In seinem Umfeld gibt es jedoch immer Personen, welche sich noch besser auf den Plattformen auskennen als

er. Es könnte sein, dass er nicht zu den 1 % aktivsten Nutzern gehört, diese jedoch seine Referenz sind und er deshalb seine Internetkompetenzen im Vergleich als gering einstuft.

Im Kapitel 4.1.4 werden die Erkenntnisse über den Vertrauenstyp 1 den anderen beiden Typen gegenübergestellt und verglichen sowie die Vertrauenstypen benannt.

4.1.2 Interpretation Vertrauenstyp 2

Dieses Kapitel widmet sich der detaillierten Analyse des Vertrauenstyps 2 und hat zum Ziel, diesen zu beschreiben. Als Erstes wird der Vertrauenstyp aufgrund der Faktoren der Clusterung analysiert, bevor er anhand demografischer Unterscheidungsmerkmale sowie der Internetnutzung charakterisiert wird.

4.1.2.1 Interpretation Vertrauenstyp 2 aufgrund der Clusterung

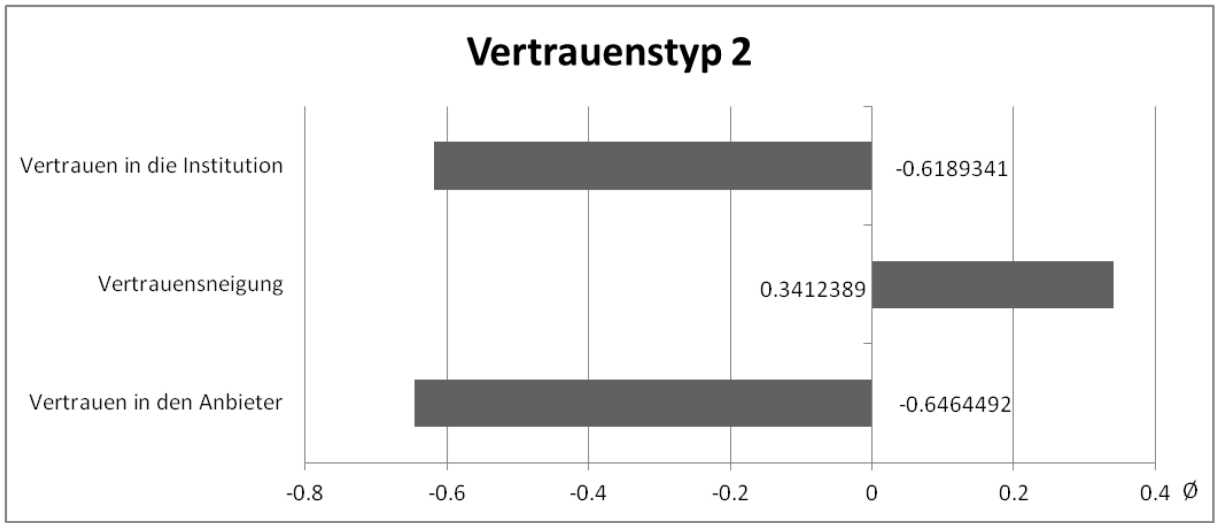


Abbildung 49: Analyse Vertrauenstyp 2 anhand des Mittelwertes Ø (Interpretation: negative Werte tendieren zu „trifft zu“, positive Werte zu „trifft nicht zu“)

Vertrauen in den Anbieter: Wie in Abbildung 49 ersichtlich, hat Vertrauenstyp 2 im Vergleich tendenziell grosses Vertrauen gegenüber seinem gewählten Anbieter (Ø -0.65). Im Anhang 7.5.4 sind die detaillierten Auswertungen des Items Vertrauen in den Anbieter für Vertrauenstyp 2 aufgeführt. Die Werte der Items liegen alle ganz klar in den Bereichen „trifft zu“ oder „trifft eher zu“. Er schätzt seinen Anbieter als wohlwollend (87.3 % „trifft zu“ oder „trifft eher zu“), kompetent (96.8 % „trifft zu“ oder „trifft eher zu“), ehrlich (94.3 % „trifft zu“ oder „trifft eher zu“), zuverlässig (97.3 % „trifft zu“ oder „trifft eher zu“), vertrauenswürdig (95.4 % „trifft zu“ oder

„trifft eher zu“) und als sympathisch (87.6 % „trifft zu“ oder „trifft eher zu“) ein. Er findet es unproblematisch, seinem Anbieter persönliche Daten zu überlassen (77.7 % „trifft zu“ oder „trifft eher zu“), und er verlässt sich voll und ganz auf die Angebotsqualität seines Anbieters (92.2 % „trifft zu“ oder „trifft eher zu“).

Vertrauenstyp 2 scheint im Vergleich mit den anderen Typen sehr von seinem Anbieter überzeugt zu sein. Dies könnte bedeuten, dass er mehr Informationen zur Abschätzung der Vertrauenswürdigkeit des Anbieters zur Verfügung hat. Es könnte sein, dass er bereits vor der Transaktion von Drittpersonen oder durch die Medien Gutes über den Anbieter gehört hat oder aber es ist eine Charaktereigenschaft von Vertrauenstyp 2, im Allgemeinen schnell zu vertrauen. Deshalb wird als Nächstes die Vertrauensneigung betrachtet.

Vertrauensneigung: Es scheint, dass Typ 2 anderen Menschen im Allgemeinen eher weniger vertraut, wie in Abbildung 49 abzulesen ist (Ø 0.34). Betrachten wir die Items der Vertrauensneigung im Detail (Anhang 7.5.5), fällt auf, dass er zwar im Allgemeinen Vertrauen zu anderen Menschen hat (50.8 % „trifft zu“ oder „trifft eher zu“), jedoch verlässt er sich nicht auf andere Menschen (77.9 % „neutral“ bis „trifft nicht zu“). Vertrauenstyp 2 hat tendenziell kein Vertrauen in die Menschheit (58.1 % „neutral“ bis „trifft nicht zu“) und findet nicht, dass Menschen generell zuverlässig sind (75.9 % „neutral“ bis „trifft nicht zu“). Anderen Menschen vertraut er, ausser es gibt Gründe, dies nicht zu tun (49.4 % „trifft zu“ oder „trifft eher zu“).

Bei der Auswertung über das vergleichsweise hohe Vertrauen in den Anbieter wurde hinterfragt, ob dieser Vertrauenstyp auch im Allgemeinen tendenziell schnell vertraut. Dies kann durch die geringe Vertrauensneigung nicht bestätigt werden. Der Vertrauensforscher Möllering fand heraus, dass bei einem eindeutigen Vertrauensmissbrauch oft nicht nur die Vertrauenswürdigkeit des anderen verloren geht, sondern aufgrund der Verunsicherung vielmehr die eigene Vertrauensbereitschaft leidet (Heidemann, 2008). Die niedrige Vertrauensbereitschaft von Typ 2 könnte demnach auf einen vergangenen Vertrauensmissbrauch hindeuten. Eine niedrige Vertrauensneigung deutet auf eine geringe Erwartungshaltung gegenüber den Mitmenschen hin (Mayer et al., 1995). Diese geringen Erwartungen könnten ein Selbstschutzmechanismus sein. Es kann sein, dass Vertrauenstyp 2 Angst davor hat, enttäuscht zu werden, und deshalb geringe Erwartungen an seine Mitmenschen hat, eine niedrige Vertrauensbereitschaft und somit eine niedrige Vertrauensneigung aufweist.

Vertrauen in die Institution: Vertrauenstyp 2 vertraut im Vergleich nicht nur seinem Anbieter, sondern in hohem Masse auch der Institution Internet (Ø -0.62) (Abbildung 49). Im Anhang 7.5.6 ist ersichtlich, dass Vertrauenstyp 2 durchgängig alle Items des Faktors Vertrauen in die Institution als für ihn zutreffend bewertet hat. Er findet, dass Online-Anbieter ihre Kunden anständig behandeln (46.4 % „trifft zu" oder „trifft eher zu"), und ist überzeugt, dass ihn Sicherheitsmechanismen (60.3 % „trifft zu" oder „trifft eher zu"), rechtliche Rahmenbedingungen (56.1 % „trifft zu" oder „trifft eher zu") sowie technische Anwendungen (71.5 % „trifft zu" oder „trifft eher zu") vor Problemen im Internet bewahren. Zudem bezeichnet er das Internet im Allgemeinen als eine stabile und sichere Umgebung (63.3 % „trifft zu" oder „trifft eher zu"). Der Vertrauenstyp 2 fühlt sich im Internet wohl und findet, dass er durch die institutionellen Rahmenbedingungen und durch die Technik vor möglichen Risiken gut geschützt ist.

Bei Vertrauenstyp 2 ist besonders interessant, dass das Vertrauen in den Anbieter wie auch in die Institution relativ hoch ist, während die generelle Vertrauensneigung vergleichsweise gering ist. Er tendiert demnach dazu, dem Internet und den Online-Anbietern zu vertrauen, nicht aber den Menschen im realen Leben. Dies könnte darauf zurückzuführen sein, dass es sich bei Transaktionen im Netz um einen Vertrag handelt, der bei Nichterfüllung sanktioniert werden kann. Diese – zum Teil öffentlichen – Sanktionierungsmöglichkeiten haben im Netz weitreichende Konsequenzen und können zum Beispiel andere Internetnutzer vor einer Transaktion mit diesem Anbieter abhalten. Aber auch rechtliche Rahmenbedingungen schützen den Nutzer bei Nichterfüllung der vereinbarten Leistung. Im realen Leben ist dies unter Privatpersonen nur bedingt möglich. Loyalität und Ehrlichkeit kann nicht per Gesetz eingefordert werden und Sanktionierungsmöglichkeiten sind nur im engeren Bekanntenkreis möglich. Dieser Unterschied könnte ein Hinweis auf die vergleichsweise geringe Vertrauensneigung des Typs 2 sein. Es könnte aber auch sein, dass sein Vertrauen in den Anbieter wie auch in die Institution von seinem gewählten Online-Geschäftsmodell abhängig ist. Die Rahmenbedingungen für das Online-Banking sind zum Beispiel reglementierter als diejenigen von sozialen Netzwerken. Dies wird unter anderem im folgenden Kapitel näher betrachtet.

4.1.2.2 Interpretation Vertrauenstyp 2 anhand demografischer Unterscheidungsmerkmale sowie der Internetnutzung

Signifikante Unterscheidungsmerkmale

In Tabelle 19 ist ersichtlich, dass sich die drei Vertrauenstypen durch Alter, höchsten Bildungsabschluss, durch das gewählte Online-Geschäftsmodell, die Nutzung sozialer Netzwerke und Online-Games sowie bezüglich der wahrgenommenen Sensibilität ihrer Daten signifikant voneinander unterscheiden.

Alter: Vertrauenstyp 2 ist im Vergleich am ältesten. Über die Hälfte (50.4 %) des Vertrauenstyps 2 ist über 46 Jahre alt und nur 17.5 % sind unter 25 jährig (Abbildung 46 & Anhang 7.5.7). Dieser Vertrauenstyp hat das Internet erst im Erwachsenenalter kennengelernt und ist nicht im digitalen Zeitalter aufgewachsen. Vertrauenstyp 2 musste sich diese Fähigkeiten neu aneignen und von Grund auf erlernen; somit gehört er zu den Digital Immigrants (Prensky, 2001; Palfrey & Gasser, 2008). Mehr als ein Fünftel (22.1 %) des Vertrauenstyps 2 ist über 66 Jahre alt und gehört somit zur Nachkriegsgeneration. Der Psychologe Largo (2011) geht davon aus, dass die Vertrauensbildung gegenüber seinen Mitmenschen besonders in den ersten Kinderjahren vom jeweiligen sozialen Umfeld geprägt wird. Die im Vergleich niedrige Vertrauensneigung könnte demnach mit den schwierigen Lebensumständen, der instabilen Werteordnung und dem erschütterten Vertrauen in die Gesellschaft erklärt werden, mit denen diese Generation aufgewachsen ist. Weiter kann angenommen werden, dass die Nachkriegsgeneration mit weniger zufrieden ist, gewohnt ist zu verzichten und zu sparen.

Man könnte annehmen, dass dieser Vertrauenstyp dem Medium Internet gegenüber eher skeptisch eingestellt ist. In Abbildung 39 ist ersichtlich, dass Vertrauenstyp 2 jedoch im Vergleich das stärkste Vertrauen in die Institution Internet aufweist. Dies könnte daran liegen, dass die Generation der Digital Immigrants Schritt für Schritt mitverfolgen konnte, wie das Internet entstand, und dadurch Vertrauen und Engagement gegenüber diesem Medium entgegenbringen. Eine denkbare Erklärung für das im Vergleich starke Vertrauen in die Institution Internet wäre aber auch der Glaube an die Technik. Technische Neuerungen haben geholfen, Deutschland wieder aufzubauen, haben das Wirtschaftswachstum gefördert und haben das Leben massiv erleichtert (Siemens, Mercedes usw.). Deshalb könnte Vertrauenstyp 2 einen starken Glauben an die Technik und somit auch in die Institution Internet aufweisen.

Bildung: Der Vertrauenstyp 2 fällt durch seinen hohen Anteil an Realschul- (20.5 %) und Berufsschulabschlüssen (23.8 %) auf (Anhang 7.5.7). Die Nachkriegsgeneration hatte weniger Möglichkeiten, sich durch Bildung frei zu entfalten, sondern es wurde tendenziell von ihr erwartet, ein solides Handwerk zu erlernen. Diese Personengruppe könnte als eher praktisch veranlagt bezeichnet werden. Nutzer dieses Vertrauenstyps interessiert es, wie ein Werkzeug beschaffen ist, wie es funktioniert – dem gehen sie mitunter in ihrem Hobbykeller auf den Grund. Praktiker sind es gewohnt, selber Hand anzulegen, und es könnte sein, dass sich dieser ältere Vertrauenstyp (Digital Immigrant) den Umgang mit dem Netz von Grund auf selbst beigebracht hat und deshalb auch ein vergleichsweise hohes Vertrauen in die Institution Internet aufweist.

Gewähltes Online-Geschäftsmodell und konkreter Anbieter: Nutzer, die dem Vertrauenstyp 2 angehören, haben sich am häufigsten bei einem Online-Shopping-Anbieter (54.2 %) oder bei einem Online-Banking-Anbieter (18.6 %) angemeldet (Abbildung 47 und Anhang 7.5.9). Beim Online-Shopping fallen insbesondere die Registrierungen bei Amazon (22.4 %) auf, aber auch diejenigen bei eBay (7.4 %), H&M (1.0 %) oder Lufthansa (0.8 %). Beim Online-Banking stechen die Registrierungen bei der Bank of Scotland (1.5 %), Commerzbank (0.8 %), ING-DiBa (0.8 %), PayPal (3.6 %) und Postbank (2.7 %) ins Auge (Abbildung 96 im Anhang 7.5.9). Online-Shopping und Online-Banking sind Bereiche, welche sensible Daten wie zum Beispiel Kreditkarteninformationen oder Kontodaten einfordern. Dies widerspiegelt das im Vergleich hohe Vertrauen in die Institution Internet und das grosse Vertrauen gegenüber dem Anbieter. Es sind aber auch beides Geschäftsmodelle, bei denen die sensiblen Daten dem Anbieter selbst und nicht der „Öffentlichkeit" zur Verfügung gestellt werden. Interessant wäre nun zu analysieren, ob das Vertrauen in den Anbieter bei der Registrierung zu einem sozialen Netzwerk ebenfalls so positiv ausfallen würde.

Nutzung von Online-Diensten (soziale Netzwerke & Online-Games): Bei der Nutzung von sozialen Netzwerken oder Online-Communitys bildet Vertrauenstyp 2 klar das Schlusslicht (Anhang 7.5.7). Obwohl die sozialen Netzwerke in Deutschland den grössten Zugang bei den über 45-Jährigen verzeichnen (Hutter, 2011), scheint dieser Vertrauenstyp noch immer untervertreten zu sein. Da es sich beim Vertrauenstyp 2 um Digital Immigrants handelt, kann angenommen werden, dass dessen soziales Umfeld ebenfalls noch nicht durchgehend auf den sozialen Netzwerken prä-

sent ist und dass dieser Typ seine Kontakte deshalb noch auf herkömmliche Art und Weise pflegt.

Interessant sind die Auswertungen im Bereich Online-Gaming: 26.1 % dieser Personengruppe nutzen Online-Games mindestens mehrmals pro Woche und Vertrauenstyp 2 ist somit Spitzenreiter im Online-Gaming (Anhang 7.5.7). Die Annahme eines Zusammenhangs zwischen Bildung und Online-Gaming kann bei diesem Vertrauenstyp bestätigt werden: Er hat das tiefste Bildungsniveau und die höchste Online-Gaming-Rate. Interessant wäre nun zu eruieren, ob die älteren Personen für diese hohe Rate verantwortlich sind und ob diese vorwiegend herkömmliche Spiele wie Poker oder Bingo online spielen oder ob sich Vertrauenstyp 2 in vernetzten, interaktiven Games engagiert. Die bisherigen Auswertungen deuten darauf hin, dass dieser Typ nicht in einer Game-Community mit sozialen Verpflichtungen eingebunden ist, sondern eher Spiele nutzt, bei denen er gegen den Computer spielt. Es kann angenommen werden, dass der etwas ältere Vertrauenstyp nicht sehr risikofreudig ist und somit eher unbezahlte Games als Freizeitbeschäftigung und aus Freude an der Technik konsumiert.

Vertrauenstyp 2 fällt durch sein vergleichsweise hohes Vertrauen in die Institution Internet und in den Anbieter, jedoch auch durch seine niedrige Vertrauensneigung auf. Es scheint, dass er sich im Internet wohlfühlt, im realen Leben aber Mühe hat, den Menschen zu vertrauen. Dies könnte ein Hinweis darauf sein, dass er aus dem realen Leben in eine perfekte virtuelle Umgebung flüchtet, welche er sich selbst kreiert. Es scheint, dass er das ganze Leben hart gearbeitet hat und nun etwas enttäuscht ist. Den Grossteil seines Lebens hat er im selben Land verbracht und ist wenig gereist. Er hat latent das Gefühl, etwas verpasst zu haben oder im Leben zu kurz gekommen zu sein und gibt seinen Mitmenschen dafür die Schuld. Die geringe Vertrauensneigung spiegelt seine geringe Erwartungshaltung gegenüber seinen Mitmenschen wider. Gleichzeitig könnte er als Vertreter der Nachkriegsgeneration einen starken Glauben an die Zukunft und in die Möglichkeiten der Technik haben, was das hohe Institutionsvertrauen erklären könnte.

Datensensibilität: Typ 2 hat in der Umfrage bei den Fragen zur Demografie und der Internetnutzung überdurchschnittlich oft keine Angaben gemacht (Anhang 7.5.10). Bei den 19 Fragen hat Typ 2 mit 14 unbeantworteten Fragen die höchste „Keine Antwort"-Rate. Besonders auffallend ist die Antwortverweigerung bei Fragen nach Alter (6.7 %), Geschlecht (3.6 %), Nutzung von Twitter (2.5 %), Nutzung von Blogs (2.3 %), Nutzung von sozialen Netzwerken/Online-Communitys (1.9 %) und

bei der Nutzung von Online TV/-Radio (1.9 %). Auch bei den Fragen, wie oft welche Online-Dienste genutzt werden, haben Personen des Vertrauenstyps 2 besonders häufig keine Antwort angekreuzt. Dies lässt darauf schliessen, dass Typ 2 extrem vorsichtig ist, dass er die abgefragten Daten als sensibel einstuft oder dass er im Allgemeinen skeptisch gegenüber der Preisgabe persönlicher Daten ist. Dies scheint jedoch beim Typ 2 nicht zuzutreffen: Bei der Aussage „Ich finde es unproblematisch, dem gewählten Anbieter persönliche Daten zu überlassen." hat er zu 77.7 % „trifft zu" oder „trifft eher zu" angekreuzt, im Gegensatz dazu ist Typ 1 diesbezüglich nur zu 28.3 % optimistisch (Anhang 7.5.4). Es scheint, dass Aussage und Verhalten bezüglich der Preisgabe seiner persönlichen Daten beim Typ 2 nicht übereinstimmen. Typ 2 kommuniziert einen unproblematischen Umgang mit persönlichen Daten, geht aber überaus restriktiv mit diesen um.

Nicht signifikante Unterscheidungsmerkmale

Tabelle 19 beinhaltet weitere, nicht signifikante Unterscheidungsmerkmale, welche für die detaillierte Beschreibung der Vertrauenstypen herangezogen werden.

Geschlecht: Die Stichprobe beim Vertrauenstyp 2 ergab eine Quote von 49.8 % weiblichen und 46.6 % männlichen Teilnehmern (3.6 % haben nichts angekreuzt). Bei diesem Vertrauenstyp sind die weiblichen Teilnehmer in der Überzahl, anhand des Geschlechtes lässt sich dieser Vertrauenstyp jedoch nicht unterscheiden (Anhang 7.5.7).

Erwerbstätigkeit und Branchen: Bei der Analyse des Bildungsniveaus haben wir gesehen, dass Vertrauenstyp 2 mit Abstand am meisten Berufsschulabschlüsse aufweist. Ausserdem ist aufgefallen, dass Vertrauenstyp 2 die älteste Gruppe ist. Deshalb erstaunt es auch nicht, dass Typ 2 mit 26.6 % überdurchschnittlich viele Rentner aufweist. Die Nachkriegsgeneration fällt insbesondere durch ihr fleissiges, arbeitswilliges und sparsames Verhalten auf. Typ 2 arbeitet vorwiegend im öffentlichen Dienst (10.5 %) oder im Gross- und Einzelhandel (6.1 %) (Anhang 7.5.7). Beruflich ist Vertrauenstyp 2 demnach eher weniger vor dem Bildschirm anzutreffen und dies lässt auf eine niedrige berufliche Internetnutzungsrate schliessen. Dies könnte ein weiterer Hinweis darauf sein, dass Vertrauenstyp 2 sich den Umgang mit dem Internet in Eigenregie beigebracht hat.

Internetnutzung: Aufgrund seiner Erwerbstätigkeit und der Branche erstaunt es, dass Typ 2 das Internet am intensivsten nutzt (tägliche Nutzung von 93 %). In Anbe-

tracht des hohen Anteils an Rentnern ergibt es wiederum Sinn, dass er das Internet mit 52.5 % vergleichsweise am meisten zu privaten Zwecken nutzt (Anhang 7.5.7). Vertrauenstyp 2 liegt jedoch bezüglich der Anzahl der Nutzerjahre im Mittelfeld (52.1 % seit mehr als acht Jahren und 22.2 % seit mehr als fünf Jahren), was die These bestätigt, dass er sich die Internetnutzung selbst beigebracht hat. Vertrauenstyp 2 gehört wahrscheinlich zu der Generation Menschen, welche bei einem neuen Produkt vor Gebrauch zuerst die Bedienungsanleitung aufmerksam durchlesen. Genauso verhält er sich im Internet, er möchte alles erkunden und verstehen und verbringt aus intrinsischer Motivation sehr viel Zeit im Internet.

Nutzung von Online-Diensten: Vertrauenstyp 2 nutzt im Vergleich am meisten unterschiedliche Online-Dienste (acht Spitzenpositionen von möglichen elf). Da er das Internet vorwiegend zu privaten Zwecken nutzt, ergibt diese Nutzungsbreite auch Sinn. Typ 2 nutzt am häufigsten jeden Tag einen E-Mail-Dienst (82.3 %) und sucht am häufigsten Informationen über Online-Dienste (91.2 % „jeden Tag“ bis „mehrmals pro Woche“). Typ 2 tätigt seine Bankgeschäfte mit Abstand am häufigsten online (56.4 % „jeden Tag“ bis „mehrmals pro Woche“), nutzt dafür aber zu 41.1 % soziale Netzwerke selten bis gar nie. Typ 2 kauft besonders häufig online ein (22.8 % „jeden Tag“ bis "mehrmals die Woche") und konsumiert auch verstärkt TV und Radio über Online-Anbieter (23.7 % „jeden Tag“ bis „mehrmals pro Woche“). Es erstaunt auch nicht, dass Typ 2 am häufigsten auf Dating-Plattformen anzutreffen ist (6.1 % „jeden Tag“ bis „mehrmals pro Woche“), am häufigsten Blogs liest (11.2 % „jeden Tag“ bis „mehrmals pro Woche“) und, wie bereits erwähnt, Online-Games nutzt (26.1 % „jeden Tag“ bis „mehrmals pro Woche“) (Anhang 7.5.7).

Interessant ist insbesondere die häufige Nutzung von Dating-Plattformen. Vertrauenstyp 2 hat eine relativ niedrige Vertrauensneigung und ist der älteste Vertrauenstyp. Es könnte sein, dass er die Dating-Plattformen als Werkzeug benutzt, um potenzielle Kandidaten im Voraus abzuschätzen zu selektieren. Es kann angenommen werden, dass sich sein soziales Umfeld in der gleichen Altersspärte befindet und er im realen Leben nicht mehr täglich neue Freunde kennenlernt. Deshalb sind Dating-Plattformen der ideale Anknüpfungspunkt für Vertrauenstyp 2.

Die hohe Nutzung von unterschiedlichen Online-Diensten widerspiegelt das im Vergleich hohe Vertrauen in die Institution Internet wie auch das grosse Vertrauen gegenüber dem Anbieter. Der Vertrauenstyp 2 hat Freude am Medium Internet, surft gerne und probiert Neues aus. Das Internet ist für ihn ein Werkzeug, ein Mittel zum Zweck, welches ihm sein Leben erleichtert. Es wurde angenommen, dass Vertrauens-

typ 2 wenig gereist ist, sich aufgrund der wirtschaftlichen Situation nicht frei entfalten konnte und er noch heute das Gefühl haben könnte, im Leben etwas zu kurz gekommen zu sein. Durch das Internet kann er jetzt zumindest teilweise nachholen; er besucht von seiner Wohnung aus spannende Länder, hört Konzerte und browst gratis durch alle deutschen Zeitungen. Er geniesst seine neue Freiheit und findet, dass früher alles mühsam erarbeitet werden musste und man sich heute mit einem Klick alles ins Haus bestellen kann. Er nutzt das Internet zur Selbstverwirklichung.

Internetkompetenzen: Vertrauenstyp 2 fällt bei der Analyse der Internetkompetenzen besonders auf. Einerseits weist er die höchste Anzahl hoher Kompetenzen auf (Spitzenreiter bei acht von zehn Fragen im Bereich „trifft zu“ und „trifft eher zu“), andererseits besitzt er die höchste Anzahl niedriger Kompetenzen (Spitzenreiter bei fünf von zehn Fragen im Bereich „trifft eher nicht zu“ und „trifft nicht zu“) (Abbildung 48 und Anhang 7.5.8). Typ 2 schätzt im Vergleich seine Kompetenzen, Informationen im Internet zu beschaffen, als hoch ein (94.9 %), ebenso seine Fähigkeit einzuschätzen, welche Informationen zuverlässig sind (79.4 %). Er findet, dass er die Qualität einer Webseite einschätzen kann (76.0 %), er ist in der Lage, ein Profil in einem sozialen Netzwerk anzulegen (65.6 %) oder Videos zu publizieren (50.7 %), kann seine Gedanken und Ideen im Internet mitteilen (54.8 %), interessiert sich für neue Entwicklungen im Internet (67.7 %) und probiert auch mal neue Online-Plattformen und Applikationen aus (40.3 %). Vertrauenstyp 2 weist eine enorme Bandbreite in Bezug auf seine Einschätzung seiner Internetkompetenzen auf und verfügt gleichzeitig über die höchsten Internetkompetenzen der drei Vertrauenstypen. Dies könnte auf seine eigenen Bemühungen zurückzuführen sein, das Internet selbst kennenzulernen, und er ist stolz darauf, dass er sich sein Wissen selbst erarbeitet hat. Diese Dynamik des stetigen Lernens gibt ihm Selbstvertrauen im Umgang mit dem Netz und spiegelt sein hohes Vertrauen in die Institution Internet wider. Ihm ist bewusst, welche Bereiche und Fähigkeiten er bereits kennt und beherrscht und welche er sich noch erarbeiten müsste. Auch bei der Analyse der Internetnutzung zeigt sich, dass Typ 2 das Internet am intensivsten nutzt (tägliche Nutzung von 93 %), dies könnte eine Erklärung für die hohen Kompetenzeinschätzungen sein. Typ 2 fällt durch sein hohes Vertrauen in die Institution Internet auf, hier kann also festgestellt werden: je höher die eigenen Internetkompetenzen, desto höher das Vertrauen in die Institution Internet.

Es könnte sein, dass besonders bei diesem Vertrauenstyp die Art und Weise der Befragung einen grossen Einfluss hatte. Würde man ältere Menschen auf der Strasse

zu ihrem Online-Verhalten befragen, würde das Ergebnis wahrscheinlich sehr unterschiedlich ausfallen. Dass durch eine Umfrage im Internet nur Onliner befragt werden können, wurde bereits im Kapitel 3.1.2 thematisiert.

Im Kapitel 4.1.4 werden diese Ergebnisse zusammengefasst, den anderen beiden Typen gegenübergestellt und die Vertrauenstypen benannt.

4.1.3 Interpretation Vertrauenstyp 3

Dieses Kapitel widmet sich der detaillierten Analyse des Vertrauenstyps 3 und hat zum Ziel, diesen näher zu charakterisieren. Zuerst wird die Interpretation aufgrund der Faktoren der Clusterung vorgenommen, um danach den Vertrauenstyp 3 aufgrund der demografischen Unterscheidungsmerkmale sowie der Internetnutzung zu beschreiben.

4.1.3.1 Interpretation Vertrauenstyp 3 aufgrund der Clusterung

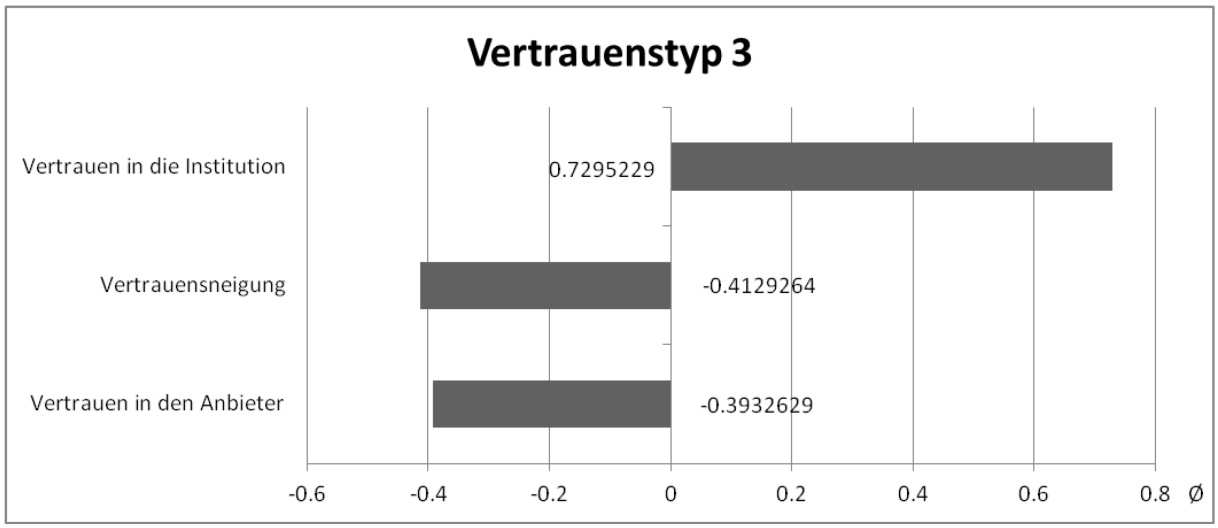


Abbildung 50: Analyse Vertrauenstyp 3 anhand des Mittelwertes Ø (Interpretation: negative Werte tendieren zu „trifft zu“, positive Werte zu „trifft nicht zu“)

Vertrauen in den Anbieter: In Abbildung 50 ist ersichtlich, dass Vertrauenstyp 3 dem Anbieter tendenziell vertraut (Ø -0.39). Im Anhang 7.5.4 sind die detaillierten Auswertungen des Items Vertrauen in den Anbieter für Vertrauenstyp 3 aufgeführt. Diese Personen haben die Items durchgehend mit entweder „trifft zu“ oder „trifft eher zu“ bewertet. Vertrauenstyp 3 schätzt seinen Anbieter als wohlwollend (79.0 %

„trifft zu“ oder „trifft eher zu“), kompetent (91.0 % „trifft zu“ oder „trifft eher zu“), ehrlich (80.6 % „trifft zu“ oder „trifft eher zu“), zuverlässig (87.6 % „trifft zu“ oder „trifft eher zu“), vertrauenswürdig (83.8 % „trifft zu“ oder „trifft eher zu“) und als sympathisch (77.6 % „trifft zu“ oder „trifft eher zu“) ein. Er findet es unproblematisch, seinem Anbieter persönliche Daten zu überlassen (64.0 % „trifft zu“ oder „trifft eher zu“), und er verlässt sich auf die Angebotsqualität seines Anbieters (84.0 % „trifft zu“ oder „trifft eher zu“). Vertrauenstyp 3 ist positiv gegenüber seinem Anbieter eingestellt und er tendiert dazu, ihm zu vertrauen.

Vertrauensneigung: Die negative Vertrauensneigung (Ø -0.41) in Abbildung 50 weist darauf hin, dass Typ 3 anderen Menschen im Allgemeinen eher vertraut. Werden die detaillierten Auswertungen des Items Vertrauensneigung für Vertrauenstyp 3 im Anhang 7.5.5 betrachtet, fällt auch hier auf, dass alle Items eher positiv bewertet wurden. Typ 3 hat im Allgemeinen Vertrauen zu anderen Menschen (78.3 % „trifft zu“ oder „trifft eher zu“), verlässt sich auf andere Menschen (33.1 % „trifft zu“ oder „trifft eher zu“), hat Vertrauen in die Menschheit (54.1 % „trifft zu“ oder „trifft eher zu“), schätzt Menschen als generell zuverlässig ein (29.7 % „trifft zu“ oder „trifft eher zu“) und vertraut Menschen, ausser es gibt Gründe, dies nicht zu tun (73.7 % „trifft zu“ oder „trifft eher zu“).

Vertrauenstyp 3 unterscheidet sich in dieser Hinsicht stark von den anderen Vertrauenstypen. Er schätzt Menschen im Vergleich als zuverlässig ein und verlässt sich auch auf diese. Dies kann bedeuten, dass er im Vergleich weniger Schwierigkeiten damit hat, Kontrolle abzugeben, mit seinen Mitmenschen zusammenzuarbeiten und zu kooperieren. Dass er an das Gute im Mensch glaubt und seinen Mitmenschen Vertrauen schenkt, könnte ein Hinweis darauf sein, dass Vertrauenstyp 3 als Teamplayer oder als Helfertyp bezeichnet werden könnte. Wenn man das Bild weiter ausführt, könnte man Vertrauenstyp 3 sogar als Idealisten bezeichnen, der das Gute im Mensch in den Vordergrund stellt.

Dieser Vertrauenstyp hat im Vergleich zu den anderen Typen eine hohe Vertrauensneigung und relativ hohes Vertrauen in Anbieter. Interessant ist nun, ob dieser Vertrauenstyp auch Vertrauen in die Institution Internet aufweist.

Vertrauen in die Institution: Vertrauenstyp 3 hat im Vergleich das geringste Vertrauen in die Institution Internet (Ø 0.73), wie in Abbildung 50 ersichtlich ist. Werden im Anhang 7.5.6 die detaillierten Auswertungen des Faktors Vertrauen in die Institution betrachtet, fällt auf, dass Vertrauenstyp 3 nicht findet, dass Online-Anbieter ihre

Kunden anständig behandeln (56.3 % „neutral“ und 27.4 % „trifft eher nicht zu“ oder „trifft nicht zu“). Des Weiteren ist Typ 3 der Meinung, dass die vorhandenen Sicherheitsmechanismen (43.0 % „trifft eher nicht zu“ oder „trifft nicht zu“) sowie die rechtlichen Rahmenbedingungen (53.9 % „neutral“ bis „trifft nicht zu“) unzureichend sind. Er vertraut hingegen den technischen Anwendungen im Netz (65.0 % „trifft zu“ oder „trifft eher zu“). Die Frage, ob er das Internet im Allgemeinen für eine stabile und sichere Umgebung halte, verneint er (75.5 % „neutral“ bis „trifft nicht zu“).

Im Vergleich zu den anderen beiden Vertrauenstypen zeigt Typ 3 deutlich am wenigsten Vertrauen in die Strukturen und Rahmenbedingungen des Internets, ist aber trotzdem darin aktiv. Er könnte das Internet als starres, gegebenes System wahrnehmen, bei welchem das Vertrauensverhältnis seiner Meinung nach sehr einseitig ist. Er ist sich gewohnt, dass er mitbestimmen und mit seinen Kollegen zusammen im Team diskutieren und entscheiden kann. Da ihm im Internet die Interaktion mit dem Mensch fehlt, fühlt er sich nicht sonderlich wohl darin.

Lee und Turban (2001) zeigen auf, dass Menschen, welche die Prozesse des Internets nicht verstehen, niedrigeres Institutionsvertrauen aufweisen. Vertrauenstyp 3 vertraut zwar den einzelnen technischen Anwendungen, er findet aber weder, dass das Internet eine stabile und sichere Umgebung ist, noch vertraut er seinen Sicherheitsmechanismen. Es könnte demnach sein, dass sich dieser Vertrauenstyp im Internet auf ihm unbekanntem Terrain bewegt und er deshalb unsicher ist. Die Unsicherheit äussert sich darin, dass er das Internet nicht als stabile Umgebung wahrnimmt oder dass er sich von den Online-Anbietern übervorteilt und nicht fair behandelt fühlt. Im folgenden Kapitel wird deshalb unter anderem die Internetnutzung und die Internetkompetenz des Vertrauenstyps 3 analysiert. Eine Erklärung dafür, dass Vertrauenstyp 3 kein Vertrauen in die Institution Internet hat, sich aber trotzdem im Netz engagiert, könnte auch sozialer Druck aus seinem Umfeld oder aber das für ihn positive Reziprozitätsverhältnis sein.

McKnight et al. (2002a) gehen davon aus, dass die wahrgenommene Zuverlässigkeit des Mediums Internet einen Einfluss auf die Nutzungsbereitschaft der User hat. Eventuell würde Vertrauenstyp 3 das Internet noch für mehr Bereiche oder das Internet öfters nutzen, wenn das institutionsbasierte Vertrauen höher wäre. Dieses vergleichsweise niedrige Institutionsvertrauen könnte auch darauf hindeuten, dass für Vertrauenstyp 3 andere Kriterien als das Institutionsvertrauen relevant sind, um sich an Transaktionen zu beteiligen. Insbesondere die Vertrauensneigung, aber auch das

Vertrauen in den Anbieter ist bei Vertrauenstyp 3 vergleichsweise stark ausgeprägt. Dies könnte bedeuten, dass dieser Vertrauenstyp nicht einem abstrakten System an sich vertraut, wohl aber den Menschen oder konkreten Anbietern. Für Vertrauenstyp 3 ist es zentral, dass reale Menschen hinter einem Angebot stehen, denen er sein Vertrauen schenken kann.

4.1.3.2 Interpretation Vertrauenstyp 3 anhand demografischer Unterscheidungsmerkmale sowie der Internetnutzung

Signifikante Unterscheidungsmerkmale

Wie in Tabelle 19 aufgeführt, unterscheiden sich die drei Vertrauenstypen durch Alter, höchsten Bildungsabschluss, durch das gewählte Online-Geschäftsmodell, die Nutzung sozialer Netzwerke und Online-Games sowie durch die wahrgenommene Sensibilität ihrer Daten signifikant voneinander.

Alter: Wie in Abbildung 46 ersichtlich, bewegt sich Vertrauenstyp 3 beim Alter im Mittelfeld. 22.2 % sind unter 25 Jahre alt und 22.0 % sind über 66-jährig (Anhang 7.5.7), die Streuung ist demnach relativ gross. Dieser Typ beinhaltet sowohl Digital Natives als auch Digital Immigrants und lässt sich durch das Alter allein schwer charakterisieren. Die Mittelfeldposition gibt aber ein Hinweis darauf, dass er sich im produktiven Alter befindet und somit noch in den Arbeitsprozess eingebunden sein müsste.

Bildung: Vertrauenstyp 3 hat zu 25.9 % ein Fachhochschul- oder Universitätsstudium, zu 18.8 % das Abitur und zu 18.8 % eine Berufsschule abgeschlossen. Somit befindet er sich auch bei der Bildung im Mittelfeld (Anhang 7.5.7). Wie bereits beim Alter lässt sich auch bei der Bildung beim Vertrauenstyp 3 keine eindeutige Tendenz feststellen, da es sich bezüglich der Bildung um einen sehr breit gestreuten Vertrauenstyp handelt.

Gewähltes Online-Geschäftsmodell und konkreter Anbieter: Vertrauenstyp 3 befindet sich bei der Registrierung zu einem neuen Online-Angebot im Vergleich zu den anderen Typen stets im Mittelfeld, wie in Abbildung 47 gut zu erkennen ist. Wird Vertrauenstyp 3 separat betrachtet, fällt auf, dass er sich mit grosser Wahrscheinlichkeit zuletzt bei einem Online-Shopping-Anbieter (50.3 %) registriert hat (Anhang 7.5.9). Auch bei der Betrachtung der konkreten Anbieter sticht Typ 3 nicht heraus (Abbildung 96 im Anhang 7.5.9). Als Online-Shopper hat er sich, noch immer

separat betrachtet, sehr häufig bei Amazon (18.0 %) und bei eBay (5.6 %) registriert. Im Vergleich zu den anderen beiden Vertrauenstypen fällt jedoch auf, dass er sich am meisten auf den sozialen Netzwerkseiten SchülerVZ, StudiVZ, MeinVZ oder Wer-kennt-wen (3.2 %) neu registriert hat. Dies sind Communitys, auf welchen sich insbesondere jüngere Internetnutzer bewegen, Typ 3 befindet sich erstaunlicherweise beim Alter aber im Mittelfeld.

Da er dem Medium Internet im Vergleich wenig Vertrauen gegenüberbringt, achtet er sehr genau auf den jeweiligen Anbieter. Es scheint, dass er beruflich wie auch privat nicht auf das Internet angewiesen ist, und er registriert sich nur bei bekannten Anbietern, von denen er bereits von Kollegen gehört hat und bei denen er sich wohlfühlt. Vertrauenstyp 3 sucht sich immer nur das heraus, was er für nötig hält, den Rest lässt er beiseite.

Nutzung von Online-Diensten (soziale Netzwerke & Online-Games): Die Analyse von Vertrauenstyp 3 bei der Nutzung von sozialen Netzwerken und Online-Communitys zeigt, dass er sich auch hier im Mittelfeld bewegt (Anhang 7.5.7). Er ist zwar auf diesen Plattformen anzutreffen und hat sich bei einigen sozialen Netzwerken registriert, es scheint jedoch, dass er sich im direkten Austausch viel wohler fühlt. Dass er sich registriert, aber nicht wirklich engagiert ist, ergibt wiederum Sinn, da er im Vergleich wenig Vertrauen in die Institution Internet hat, er aber gerne mit dabei sein will, um im realen Leben mitreden zu können. Da es sich bei Vertrauenstyp 3 sowohl um Digital Natives als auch um Digital Immigrants handelt, macht diese mittlere Platzierung nochmals Sinn.

Bei der Nutzung von Online-Games jedoch ist Vertrauenstyp 3 im Vergleich zu den anderen Typen klar das Schlusslicht (Anhang 7.5.7). Vertrauenstyp 3 ist somit sicherlich kein Gamer-Typ. Er möchte mit seinen Kollegen gemeinsam an einem Tisch sitzen und bei einer Partie Poker einen schönen Abend geniessen, sicherlich aber nicht den Abend alleine zuhause vor dem Computer verbringen. Bei den vorhergehenden Typenbetrachtungen wurde hinterfragt, ob eventuell die Bildung einen Einfluss auf das Gaming-Verhalten hat. Dies konnte bei Vertrauenstyp 3 nicht bestätigt werden, da er bei der Bildung im Mittelfeld liegt und im Vergleich wenig auf Online-Gaming-Plattformen anzutreffen ist.

Datensensibilität: Auf die Aussage „Ich finde es unproblematisch, dem gewählten Anbieter persönliche Daten zu überlassen." hat Vertrauenstyp 3 mit 64 % „trifft zu" oder „trifft eher zu" geantwortet und liegt somit auch hier im Mittelfeld (An-

hang 7.5.4). Auch bei der Auswertung seiner „Keine Antwort"-Rate bei den Fragen zur Demografie und der Internetnutzung befindet sich Typ 3 im Mittelfeld (Anhang 7.5.10). Beim Vertrauenstyp 3 stimmt seine Aussage über die Handhabung seiner persönlichen Daten mit seinem Verhalten überein.

Nicht signifikante Unterscheidungsmerkmale

Tabelle 19 beinhaltet weitere, nicht signifikante Unterscheidungsmerkmale der drei Cluster, welche für die detaillierte Beschreibung der Vertrauenstypen herangezogen werden.

Geschlecht: Vertrauenstyp 3 besteht zu 50.1 % aus weiblichen und zu 46.7 % aus männlichen Teilnehmern (3.2 % haben nichts angekreuzt) (Anhang 7.5.7). Bei diesem Typ sind die weiblichen Teilnehmer im Verglich zum Gesamtsample und zu den anderen beiden Personengruppen in der Überzahl.

Erwerbstätigkeit und Branchen: Dieser Typ arbeitet mit 39.5 % am häufigsten als Angestellter, insbesondere im öffentlichen Dienst (10.6 %) oder im Gesundheits- und Sozialwesen (6.4 %) (Anhang 7.5.7). Für diese Berufe wird eine fundierte, solide Bildung vorausgesetzt, ein hoher akademischer Grad ist nicht notwendig. Dies könnte ein Hinweis auf die Mittelfeldposition im Bildungsbereich sein. Vertrauenstyp 3 befindet sich im produktiven Alter und könnte ein kleines Team führen. Menschen, welche im öffentlichen Dienst oder im Gesundheits- und Sozialwesen arbeiten, haben oft direkten Kontakt zu Menschen und arbeiten weniger am Computer. Deshalb interessiert hier insbesondere die Vertrauensneigung des Vertrauenstyps 3, welche vergleichsweise stark ausgeprägt ist und auf grosses Vertrauen gegenüber anderen Menschen hindeutet. Vertrauenstyp 3 ist am Wohl seiner Mitmenschen interessiert und es scheint, dass Vertrauenstyp 3 dann erfüllt ist, wenn er mit Menschen zusammenarbeiten kann. Auch scheint es, dass für sein Engagement weniger monetäre Anreize im Vordergrund stehen, sondern soziale Anerkennung. Die soziale Anerkennung durch sein Umfeld ist ihm durch sein Engagement im sozialen Bereich gesichert. Im Netz hingegen ist ihm Anerkennung weniger wichtig, er sucht Bestätigung in seinem realen Umfeld.

Bei der Analyse des gewählten Online-Geschäftsmodells und des konkreten Anbieters ist Vertrauenstyp 3 besonders durch seine Registrierungen auf den sozialen Netzwerkseiten SchülerVZ, StudiVZ, MeinVZ oder Wer-kennt-wen aufgefallen – alles Seiten für ein tendenziell jüngeres Publikum. Es könnte sein, dass er durch sei-

nen Beruf oft mit jungen Menschen zusammenarbeitet und er sich auch deshalb gezwungen sieht, sich im Internet wenigstens Grundkenntnisse anzueignen, wozu seiner Meinung nach auch die Zugehörigkeit zu einem der oben genannten sozialen Netzwerkseiten gehört.

Internetnutzung: Typ 3 nutzt das Internet von allen Typen am wenigsten intensiv (tägliche Nutzung von 90.8 %), dafür liegt er bei der Interneterfahrung ganz vorn: 58.7 % nutzen das Internet seit mehr als acht Jahren. Dies ist interessant, da es sich bei diesem Vertrauenstyp nicht um besonders junge Probanden handelt, die das Internet bereits seit Kindertagen und somit seit vielen Jahren nutzen. Vertrauenstyp 3 befindet sich in Bezug auf das Alter im Mittelfeld, und deshalb erstaunt die Spitzenreiterrolle bei der Interneterfahrung. Dies könnte ein Hinweis auf die Technikbegeisterung des Vertrauenstyps 3 sein. Diese Annahme wird jedoch dadurch entkräftet, dass Nutzer dieses Vertrauenstyps das Internet im Vergleich am wenigsten intensiv nutzen. Die tiefe Nutzungsrate könnte jedoch mit der Branche zusammenhängen, in der Vertreter des Vertrauenstyps 3 vorwiegend tätig sind. Im öffentlichen Dienst wie auch im Gesundheits- und Sozialwesen arbeitet man eher weniger am Computer, was auch den Durchschnittswert sowohl bei der beruflichen als auch bei der privaten Nutzung (48.7 %) des Internets erklärt (Anhang 7.5.7). Es scheint, dass dieser Vertrauenstyp das Internet schnell adaptiert hat, sich jedoch nicht zum Internet-Euphoriker weiterentwickelt hat. Diesem Vertrauenstyp sind sein soziales Umfeld und sein Status in diesem Umfeld im realen Leben besonders wichtig. Er möchte mit seinen Internetaktivitäten nicht völlig im Abseits liegen, weshalb er sich für die Teilnahme und Nutzung entscheidet. Er möchte mitreden, dabei sein und teilhaben, obwohl er selbst kein tiefes Interesse für Internetaktivitäten mitbringt. Vertrauenstyp 3 nimmt keine Vorreiterrolle ein, er fällt nicht durch sein Engagement auf und ist nie der Erste, der einen neuen Anbieter ausprobiert. Wenn er jedoch viel über einen Anbieter hört, registriert er sich umgehend, bleibt jedoch ein eher passiver Nutzer.

Nutzung von Online-Diensten: Typ 3 nutzt am wenigsten „jeden Tag“ seine E-Mails (78.4 %) und sucht auch seine Informationen am wenigsten häufig online (86.8 % „jeden Tag“ bis „mehrmals die Woche“). Des Weiteren fällt auf, dass Typ 3 eher weniger online einkauft (27.3 % „selten“ bis „nie“) und auch TV und Radio nur äusserst selten online konsumiert (17.6 % „jeden Tag“ bis „mehrmals die Woche“). Typ 3 ist tendenziell selten auf Dating-Plattformen (89.8 % „selten“ bis „nie“), auf Microblogs (87.2 %) und Blogs (76.5 %) oder bei Online-Games (60.7 %) anzutreffen (Anhang 7.5.7). Vertrauenstyp 3 nutzt insgesamt auffallend wenig oft Online-Dienste

im Vergleich zu den anderen Typen (null Spitzenpositionen von möglichen elf). Dieses Ergebnis stimmt mit der niedrigen täglichen Internetnutzungsrate überein und bestätigt das kaum vorhandene Vertrauen in die Institution Internet von Vertrauenstyp 3.

Wie bereits bei den Auswertungen des Online-Geschäftsmodells und bei der Nutzung von sozialen Netzwerken und Online-Games festgestellt, nutzt Vertrauenstyp 3 wenige Online-Dienste, bei welchen er sich mit seinen persönlichen Daten exponieren müsste. Er liest und informiert sich, ist aber nicht aktiv an der Konversation in den Sozialen Medien beteiligt und es scheint, dass er bis jetzt keine negativen Erfahrungen in Bezug auf seine Daten gemacht hat. Es könnte sein, dass er aus diesem Grund kein offenes Ohr für Datenschutzskandale und Systempannen der Anbieter hat und dadurch sein im Vergleich hohes Vertrauen in den Anbieter erklärt werden könnte.

Internetkompetenzen: Vertrauenstyp 3 befindet sich bei der Einschätzung seiner Internetkompetenzen klar im Mittelfeld (Abbildung 48 und Anhang 7.5.8). Nur bei der Frage, ob er Informationen auf einem Blog oder bei Twitter veröffentlichen kann, ist er im Vergleich Spitzenreiter (49.7 % „trifft zu“ oder „trifft eher zu“). Diese Einschätzung ist interessant, denn bei der Nutzung von Blogs und Twitter hat Vertrauenstyp 3 angegeben, dass er Blogs (76.5 % „trifft eher nicht zu“ oder „trifft nicht zu“) und Twitter (87.2 „trifft eher nicht zu“ oder „trifft nicht zu“) im Vergleich zu den anderen Typen am wenigsten nutzt. Wenn er wollte, könnte er Informationen veröffentlichen, er macht es aber nicht. Vertrauenstyp 3 fühlt sich auffallend häufig nicht in der Lage, ein Profil in einem sozialen Netzwerk anzulegen (19.4 % „trifft eher nicht zu“ oder „trifft nicht zu“). Betrachten wir die Nutzung von sozialen Netzwerken, wird bestätigt, dass er diese am wenigsten häufigsten nutzt (nur 41.4 % „jeden Tag“ oder „mehrmals pro Woche“). Die mässigen Internetkompetenzen von Vertrauenstyp 3 könnten mit seiner im Vergleich wenig intensiven Internetnutzung (tägliche Nutzung von 90.8 %) und seiner Tätigkeit im öffentlichen Dienst oder im Gesundheits- und Sozialwesen zusammenhängen. Bei der Analyse des Institutionsvertrauens wurde auf die Ergebnisse von Lee und Turban (2001) hinsichtlich Vertrautheit mit dem Internet und Vertrauensbereitschaft hingewiesen. Vertrauenstyp 3 bestätigt diese Forschungsergebnisse grösstenteils: Nutzer des Vertrauenstyps 3 bewegen sich im Netz auf unbekanntem Terrain und verstehen eventuell die Prozesse dahinter nicht und weisen, wie prognostiziert, das geringste Vertrauen aller Typen in die Institution Internet auf.

Vertrauenstyp 3 fällt im Allgemeinen durch seine häufige Tendenz zur goldenen Mitte auf. Der Mittelweg lässt sehr viel Spielraum zu beiden Seiten. Es könnte sein, dass dieser Vertrauenstyp schwer zu greifen ist, da für ihn die reale Welt zentral ist und das Internet heute einfach nur dazugehört. Das Internet hat für ihn eine geringe Relevanz und die Internetnutzung ist für ihn keine bewusste Entscheidung, sondern ein Weg zu dem Ziel, in seinem realen Umfeld mitreden zu können.

Im folgenden Kapitel 4.1.4 werden diese Ergebnisse mit den anderen beiden Typen verglichen und die drei Vertrauenstypen benannt.

4.1.4 Gegenüberstellung und Benennung der drei Vertrauenstypen

In Tabelle 20 werden die Vertrauenstypen einander gegenübergestellt und aufgrund der signifikanten Unterscheidungsmerkmale diskutiert.

	Vertrauenstyp 1	**Vertrauenstyp 2**	**Vertrauenstyp 3**
Signifikante Unterscheidungsmerkmale			
Vertrauen in den Anbieter	Im Vergleich niedriges Vertrauen in den Anbieter (Ø 1.02)	Im Vergleich hohes Vertrauen in den Anbieter (Ø -0.65)	Vertraut dem Anbieter im Vergleich (Ø -0.39)
Vertrauensneigung	Neigung, anderen zu Vertrauen neutral (Ø 0.05)	Vertraut anderen im Allgemeinen wenig (Ø 0.34)	Vertraut anderen im allgemeinen stark (Ø -0.41)
Vertrauen in die Institution	Vertraut der Institution Internet im Vergleich mässig (Ø -0.07)	Vertraut der Institution Internet im Vergleich (Ø -0.62)	Im Vergleich niedriges Vertrauen in die Institution Internet (Ø 0.73)
Alter	Eher jünger	Eher älter	Mittelfeld
Bildung	Gut gebildet oder noch in Ausbildung	Viele Realschul- & Berufsschulabschlüsse	Mittelfeld
Online-Geschäftsmodell & konkreter Anbieter	Soziale Netzwerke (Facebook) & Anbieter von Online-Informationen (Google, YouTube)	Anbieter von Online-Shopping- (Amazon, eBay, H&M & Lufthansa) & Online-Banking (Bank of Scotland, Commerzbank, ING-DiBa, PayPal, Postbank)	Mittelfeld
Nutzung von Online-Geschäftsmodellen	Nutzt auffallend oft soziale Netzwerke	Nutzt auffallend oft Online-Games	Nutzung von sozialen Netzwerken im Mittelfeld, nutzt fast nie Online-Games
Datensensibilität	Niedrigste „Keine Antwort"-Rate, Privacy-Paradox: Diskrepanz zwischen Aussage & Verhalten	Höchste „Keine Antwort"-Rate, restriktive Daten-Handhabung	Mittelfeld
Nicht signifikante Unterscheidungsmerkmale			
Geschlecht	Eher männlich	keine Differenzierung beim Geschlecht	Eher weiblich
Erwerbstätigkeit & Branche	Angestellter oder noch in Ausbildung, häufig im Gesundheits- & Sozialwesen tätig	Rentner oder Angestellter, häufig im öffentlichen Dienst/Gross- & Einzelhandel tätig	Angestellter, arbeitet vorwiegend im öffentlichen Dienst/Gesundheits- & Sozialwesen
Internetnutzung	Tägliche Nutzung im Mittelfeld, kurze Nutzungserfahrung in Jahren, niedrigste private Nutzungsrate	Höchste tägliche Nutzung, Nutzungserfahrung in Jahren im Mittelfeld, höchste private Nutzungsrate	Niedrigste tägliche Nutzung, höchste Nutzungserfahrung in Jahren, private Nutzungsrate im Mittelfeld
Nutzung von Online-Diensten	Nutzung von Online-Diensten im Mittelfeld (3 Spitzenpositionen von 11)	Nutzt am meisten unterschiedliche Online-Dienste (8 Spitzenpositionen von 11)	Nutzt am wenigsten oft unterschiedliche Online-Dienste (0 Spitzenpositionen von 11)
Internetkompetenzen	Geringste Internetkompetenzen	Höchste Internetkompetenzen	Mittelfeld

Tabelle 20: Gegenüberstellung der drei Vertrauenstypen

Vertrauenstyp 1 hat im Vergleich das niedrigste Vertrauen in den Online-Anbieter und schätzt seine Bereitschaft, anderen Menschen im realen Leben zu vertrauen, tendenziell neutral bis negativ ein. Interessant ist, dass er überzeugt ist, sich auf andere verlassen zu können, es aber selbst nicht macht. Vertrauenstyp 1 scheint ein selekti-

ver Mensch zu sein, der viel Wert auf Souveränität legt, und er will die Kontrolle selbst in der Hand haben. Er könnte als Einzelkämpfer oder Individualist bezeichnet werden, welcher skeptisch gegenüber Einflüssen von aussen ist. Auch dem Internet als Institution vertraut er im Vergleich nur zögerlich. Dass das Internet durch eine Vielzahl von Personen und Institutionen gesteuert und kontrolliert wird, gibt ihm jedoch ein Mindestmass an Sicherheit. Dies könnte als Indiz dafür gesehen werden, dass er der Weisheit der Vielen grossen Wert beimisst. Vertrauenstyp 1 ist im Vergleich relativ jung und es scheint sich bei Nutzern des Vertrauenstyps 1 somit vorwiegend um Digital Natives zu handeln, welche bereits mit der Technologie aufgewachsen sind und ein entspanntes Verhältnis zum Internet haben. Typ 1 ist mit dem Medium vertraut, betrachtet das Internet jedoch auch kritisch und hinterfragt es. Er ist sehr gut gebildet oder noch immer in Ausbildung und scheint eher der kopflastige Typ zu sein, welcher bei zu vielen Emotionen unsicher wird. Vertrauenstyp 1 ist ein häufiger Nutzer von sozialen Netzwerken und Communitys und er tendiert dazu, sein soziales Umfeld lieber online zu pflegen. Dass er wenig Vertrauen in den Anbieter hat, kann mit seinem gewählten Anbieter Facebook erklärt werden, welcher für seine Datenschutzpraktiken immer wieder öffentlich kritisiert wird. Sein Wissensbedürfnis stillt er durch Anbieter von Informationsplattformen. Es scheint, dass er mit seinen privaten Daten relativ freizügig umgeht, obwohl er von sich selbst sagt, dass er seine Daten restriktiv verwaltet. Diese Diskrepanz zwischen seiner Aussage und seinem Verhalten kann mit dem Privacy-Paradox (Kapitel 2.2.2.2) erklärt werden: Wenn der wahrgenommene Nutzen einer Offenlegung privater Daten höher ist als die wahrgenommenen eingegangenen Risiken, werden private Daten im Internet trotz Privacybedenken offengelegt. Aufgrund seines vergleichsweise niedrigen Vertrauens in den Anbieter und in die Menschen, seinem zögerlichen Vertrauen in die Institution Internet, seiner kritischen und hinterfragenden Haltung gegenüber dem Internet und aufgrund seines Bedürfnisses nach Information und Kontrolle wird dieser Vertrauenstyp als Skeptiker bezeichnet (Abbildung 51).

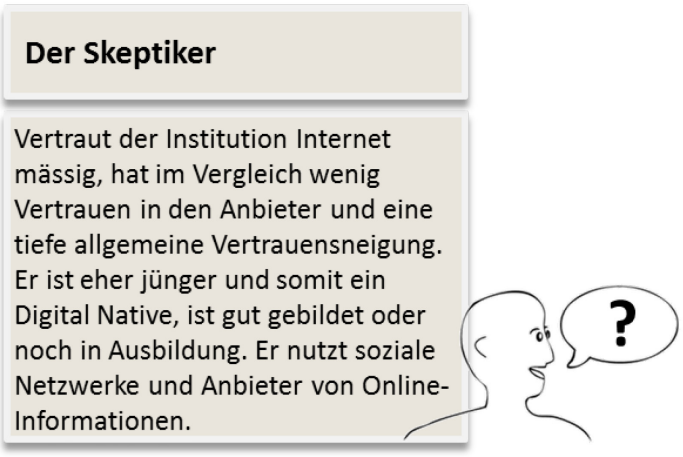


Abbildung 51: Der Skeptiker (eigene Darstellung)

Vertrauenstyp 2 hat im Vergleich hohes Vertrauen gegenüber dem Anbieter. Schnell zu Vertrauen scheint jedoch keine Charaktereigenschaft von Typ 2 zu sein, seine Vertrauensneigung ist gering, er besitzt im Vergleich die niedrigste allgemeine Vertrauensbereitschaft, was auf eine geringe Erwartungshaltung gegenüber seinen Mitmenschen hinweist. Dem Internet als Institution vertraut er jedoch in vergleichsweise hohem Mass. Es scheint, dass Vertrauenstyp 2 dem Internet und den Online-Anbietern vertraut, nicht aber den Menschen im realen Leben. Dieser Typ könnte sich in der Internet-Umgebung wohler fühlen als in der realen Welt. Vertrauenstyp 2 ist im Vergleich am ältesten, zu ihm zählen sich vorwiegend Digital Immigrants, welche nicht mit dem Internet aufgewachsen sind. Es kann angenommen werden, dass sich dieser Vertrauenstyp seine Fähigkeiten im Umgang mit dem Internet selbst erarbeitet hat. Er fällt durch seinen hohen Anteil an Realschul- und Berufsschulabschlüssen auf und könnte als eher praktisch veranlagt bezeichnet werden. Vertrauenstyp 2 hat sich am häufigsten bei einem Online-Shopping-Anbieter oder bei einem Online-Banking-Anbieter angemeldet, nutzt äusserst selten Online-Communitys, dafür ist er Spitzenreiter bei der Nutzung von Online-Games. Er weist eine restriktive Datenhandhabung auf und will wissen, wo und wann er welche Daten von sich preisgibt. Das Internet ist für Vertrauenstyp 2 mit einem Werkzeug zu vergleichen, welches er als Mittel zum Zweck nutzt. Weiter deutet die Häufung bei den Berufsschulabschlüssen auf einen Mensch hin, der gerne selbst Hand anlegt. Vertrauenstyp 2 wird deshalb als Praktiker bezeichnet (Abbildung 52).

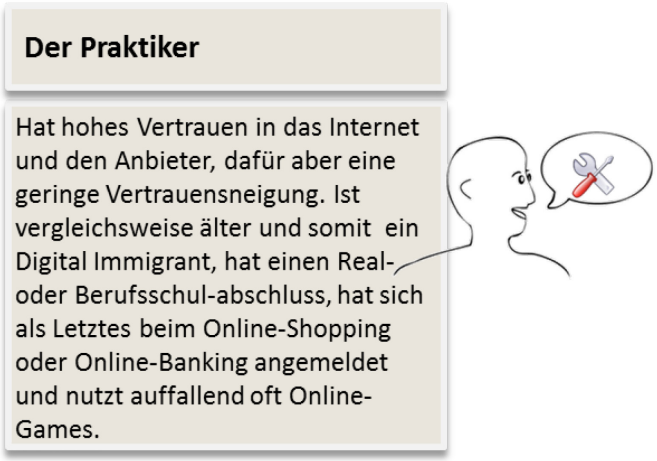


Abbildung 52: Der Praktiker (eigene Darstellung)

Vertrauenstyp 3 ist positiv gegenüber seinem Anbieter eingestellt und bereit, diesem zu vertrauen. Vertrauenstyp 3 schätzt Menschen im Vergleich als zuverlässig ein und verlässt sich auch auf diese. Er hat die am stärksten ausgeprägte Vertrauensneigung und es scheint, dass dieser Typ ein Idealist ist, der an das Gute im Mensch glaubt. Man kann annehmen, dass er Kontrolle gerne in der Gruppe wahrnimmt und eher ein Teamplayer ist. Gleichzeitig weist er im Vergleich das geringste Vertrauen in die Institution Internet, in ihre Strukturen und Rahmenbedingungen auf. Vertrauenstyp 3 bewegt sich im Netz tendenziell auf ihm unbekanntem Terrain und könnte deshalb unsicher sein. Es scheint, dass er nicht einem abstrakten System an sich vertrauen kann, sondern dass es für ihn zentral ist, reale Menschen hinter einem Angebot zu sehen, denen er sein Vertrauen schenken kann. Für Vertrauenstyp 3 stehen demnach die Menschen klar im Vordergrund und er verlässt sich lieber auf Menschen als auf Maschinen. Vertrauenstyp 3 umfasst sowohl Digital Natives als auch Digital Immigrants. Ebenso divers und breit gestreut sind die Bildungsabschlüsse, welche vom Berufsschul- bis zum Universitätsabschluss gehen. Der Vertrauenstyp 3 sticht auch beim gewählten Online-Geschäftsmodell und beim Gebrauch von sozialen Netzwerken nicht hervor, er befindet sich immer in der goldenen Mitte. Beim Online-Gaming-Verhalten jedoch liegt er ganz klar im Hintertreffen, Typ 3 ist somit kein Online-Gamer. Ganz allgemein befindet er sich auffallend häufig in der Mittelfeldposition. Da Vertrauenstyp 3 an das Gute im Menschen glaubt und im Vergleich eine ausgeprägte Vertrauensneigung aufweist, dem Anbieter gegenüber Vertrauen entgegenbringt und ihm Beziehungen mit realen Menschen wichtig sind, wird Vertrauenstyp 3 als der Soziale bezeichnet (Abbildung 53).

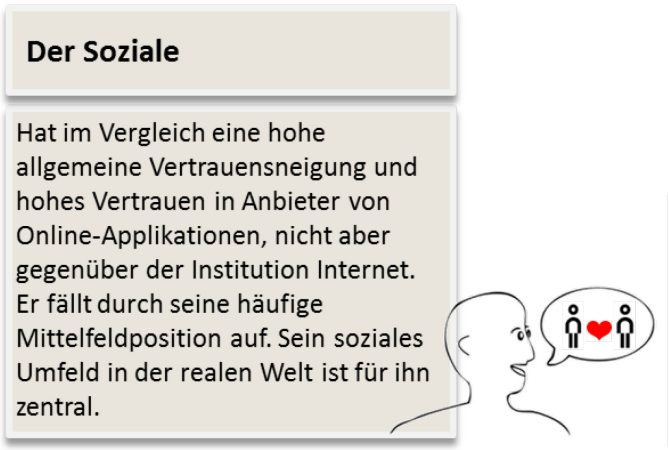


Abbildung 53: Der Soziale (eigene Darstellung)

Der Praktiker und der Soziale leben beide in der Offline-Welt und tätigen einzelne Transaktionen im Internet. Das Internet dient ihnen als Werkzeug, als Weg zum Ziel. Beim Skeptiker hingegen sind diese beiden Welt fest miteinander verflochten.

Die erste Forschungsfrage „Existieren bei Internetnutzern unterschiedliche Vertrauenstypen?“ kann demnach klar bejaht werden. Es konnten drei Vertrauenstypen unterschieden werden, welche sich im Hinblick auf ihr Vertrauen in den Anbieter, ihre Vertrauensneigung, ihr Vertrauen in die Institution unterscheiden. Ausserdem können die drei Vertrauenstypen anhand demografischer Faktoren, Auswertungen zur Internetnutzung sowie hinsichtlich ihrer Internetkompetenzen und der Einschätzung der Sensibilität der Daten differenziert werden. Die drei Vertrauenstypen sind der Skeptiker, der Praktiker und der Soziale.

Im nächsten Kapitel werden die drei Vertrauenstypen auf ihr Verhalten während einer Transaktion hin untersucht. Ausserdem wird analysiert, auf welche Vertrauensfaktoren sie achten.

4.2 Jeder achtet auf andere Indikatoren: Relevante Vertrauensfaktoren pro Vertrauenstyp

Dieses Kapitel widmet sich der detaillierten Analyse und Beantwortung der zweiten Forschungsfrage: „Sind während einer Transaktion im Internet für die unterschiedlichen Vertrauenstypen dieselben Vertrauensfaktoren relevant?“ Im vorhergehenden Methodik-Kapitel 3.1.2 haben wir durch den Kruskal-Wallis-Test (Tabelle 15, S. 137) die vier Vertrauensfaktoren Reziprozität, Marke und Design, Nutzerkontrolle und Kundenservice bestimmt, welche sich pro Vertrauenstyp signifikant unterscheiden. Die Faktoren Proaktive Kommunikation sowie Technik wurden durch die Faktorenanalyse nicht bestätigt und die Vertrauensfaktoren Realweltbezug und Empfehlungen weisen keine Signifikanz auf und wurden von weiteren Analysen ausgeschlossen. Um zu verdeutlichen, wie Anbieter von Online-Geschäftsmodellen diese Vertrauensfaktoren auf den jeweiligen Vertrauenstyp abstimmen können, wurden bei jedem Faktor aktuelle Beispiele verwendet. Zuerst wird im Kapitel 4.2.1 der Skeptiker (Vertrauenstyp 1) diskutiert, im Kapitel 4.2.2 wird der Praktiker (Vertrauenstyp 2) und im Kapitel 4.2.3 der Soziale (Vertrauenstyp 3) im Detail besprochen.

Da der Skeptiker im Vergleich auf keine der vier identifizierten Vertrauensfaktoren achtet, werden bei diesem Vertrauenstyp ausnahmsweise direkt die einzelnen Items betrachtet. Beim Praktiker und beim Sozialen hingegen werden die Mittelwerte der vier Faktoren miteinander verglichen.

4.2.1 Relevante Vertrauensfaktoren für den Skeptiker (Vertrauenstyp 1)

Dieses Kapitel befasst sich mit den im Methodik-Kapitel 3.2.1 identifizierten relevanten Vertrauensfaktoren für den Skeptiker (Vertrauenstyp 1). Der Mittelwertvergleich (Tabelle 16) hat aufgezeigt, dass der Skeptiker während einer Transaktion im Vergleich am wenigsten auf die untersuchten Vertrauensfaktoren achtet, wie in Abbildung 54 grafisch dargestellt ist.

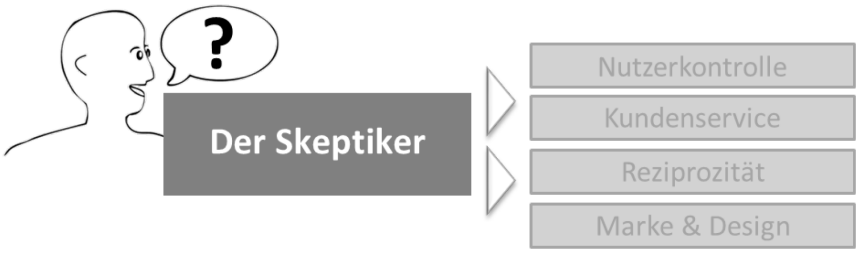


Abbildung 54: Relevante Vertrauensfaktoren für den Skeptiker (Vertrauenstyp 1) (eigene Darstellung)

Bei der Auswertung der Vertrauenstypen haben wir gesehen, dass der Skeptiker gerne Kontrolle über sein Umfeld hat. Es scheint, dass es für Vertrauenstyp 1 wichtig ist, dass er souverän ist, selbst entscheiden kann und dabei nicht beeinflusst wird. Jeglicher Beeinflussung von aussen steht er kritisch bis abwehrend gegenüber. Da erstaunt es nicht, dass der Skeptiker von sich sagt, dass er sich ungern auf vom Unternehmen konstruierte Marken oder auf aufwändig gestaltetes Design einer Website verlässt (Ø .370). Auch Kosten-Nutzen-Überlegungen (Ø .310) scheinen ihn in seinem Entscheid im Vergleich weniger zu beeinflussen. Als Einzelkämpfer möchte er nicht abwägen müssen, insbesondere nicht im Team, sondern er ist der Entscheider und wenn er sich für ein Angebot entschieden hat, steht das fest. Da er eher negativ auf Beeinflussungsversuche reagiert, nimmt er nur widerwillig mit dem Unternehmen Kontakt auf, weshalb ihn auch ein gut vermarkteter Kundenservice nicht dazu veranlasst, einem Unternehmen zu vertrauen (Ø .310). Ausserdem scheint es so zu sein, dass ihm im Vergleich weniger wichtig ist, wie seine persönlichen Daten bei einem Unternehmen gehandhabt werden und wer genau die Kontrolle über diese Daten besitzt (Ø .059). Dies ergibt beim Skeptiker eigentlich wenig Sinn, da er wissbegierig ist, viel Wert auf Souveränität legt und sein Schicksal selbst in den Händen halten will. Der Skeptiker legt tendenziell viel Wert auf Unabhängigkeit und lässt sich nicht gerne festlegen. Ihm widerstrebt es, wenn er von aussen beeinflusst wird und er möchte jede Fremdbestimmung von Anfang an vermeiden. Dies lässt erwarten, dass der Faktor Kontrolle überaus wichtig für den Skeptiker ist, was aber nicht der Fall zu sein scheint. Dies könnte aufgrund seiner Abwehrhaltung erklärt werden: Obwohl er zum Kontrollmensch tendiert, will er selbstbestimmt jedes Mal aufs Neue frei entscheiden können. Er würde nie eingestehen, dass er sich zum Beispiel durch für ihn günstige AGBs verleiten lassen würde. Aufgrund seiner skeptischen bis misstrauischen Art, seiner geringen Internetkompetenzen oder seinen beruflichen Erfahrun-

gen hat er Angst vor potenziellen Verletzungen oder Abhängigkeiten, schottet sich ab und sagt, dass er während einer Transaktion im Netz tendenziell auf keine der vier untersuchten Faktoren achtet.

In der vorhergehenden Analyse der Vertrauenstypen (Kapitel 4.1.1) wurde festgestellt, dass der Skeptiker das Internet eher für einzelne, spezifische Dienste nutzt und dann in jedem Fall einzeln beurteilt, ob er dem Anbieter vertraut oder nicht. Er probiert gerne Neues aus und klickt sich durch. Er gehört nicht zu der Generation Menschen, welche eine Gebrauchsanleitung durchlesen, sondern für ihn muss eine Seite oder ein Tool intuitiv bedienbar sein. Es könnte sein, dass sich der Digital Native im Internet auf sicherem Terrain bewegt, dass er in eine Seite eintaucht und nur das Gesamtbild wahrnimmt. Seine digitale Intuition warnt ihn, wenn etwas nicht stimmig ist. Anhand welcher Faktoren der Skeptiker dies jedoch beurteilt, kann aufgrund der getesteten Faktoren nicht beurteilt werden. Diese Analyse schliesst jedoch aus, dass der Skeptiker im Vergleich stark auf die Faktoren Reziprozität, Marke und Design, Nutzerkontrolle oder Kundenservice achtet. Um diesen Vertrauenstyp und dessen Verhalten etwas greifbarer zu machen, werden ausnahmsweise direkt die einzelnen Items der vier Faktoren betrachtet und besonders auffällige Antwortstrukturen des Skeptikers hervorgehoben (siehe Abbildung 55). Anhand von konkreten Beispielen wird nun aufgezeigt, wie auf die Bedürfnisse des Skeptikers eingegangen werden könnte.

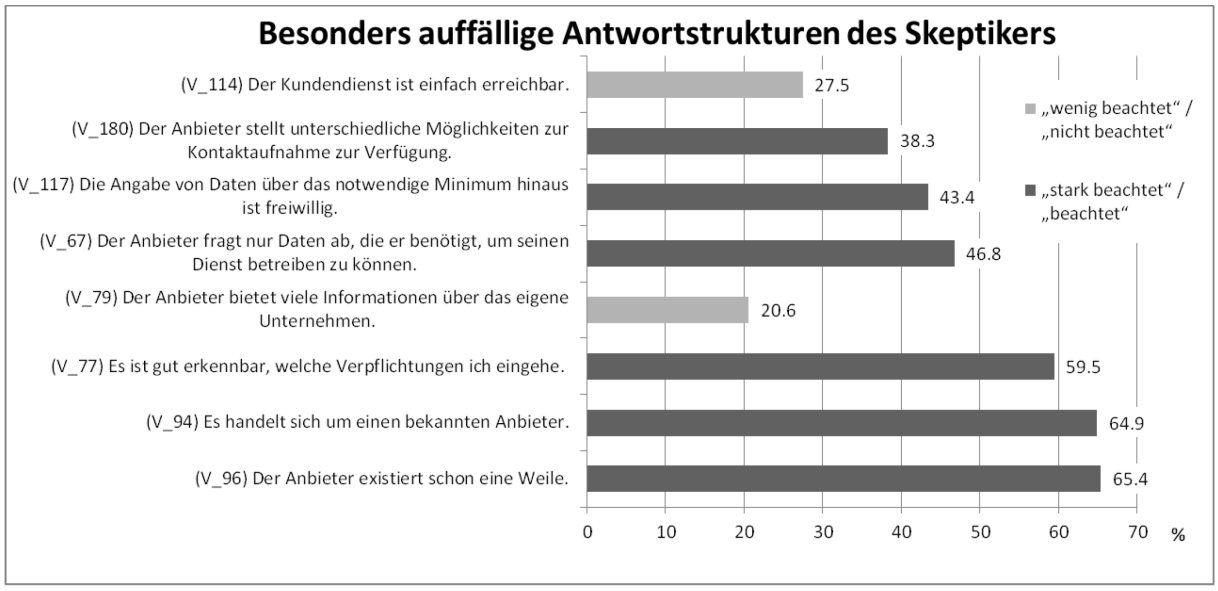


Abbildung 55: Besonders auffällige Antwortstrukturen des Skeptikers (eigene Darstellung)

Es scheint, dass Kontinuität dem Skeptiker Sicherheit vermittelt. Er achtet darauf, ob der Anbieter bereits eine Weile existiert oder nicht (V_96, 65.4 % „stark beachtet“ oder „beachtet“). Im Vergleich zu den anderen beiden Typen ist die Kontinuität beim Skeptiker jedoch am wenigsten stark ausgeprägt. Weiter achtet er darauf, ob es sich um einen bekannten Anbieter handelt (V_94, 64.9 % „stark beachtet“ oder „beachtet“, Anhang 7.6.3). Alter und Bekanntheit sind demnach Indikatoren, welche für den Skeptiker zur Beurteilung der Vertrauenswürdigkeit dienen. Das Auktionshaus Ricardo macht beispielsweise mithilfe des Komikers Beat Schlatter Werbung mit dem Slogan: „Willkommen im grööööössten Shopping-Center der Schweiz!“ (Ricardo, 2012). Bei der Suche über die Suchmaschine Google ist bei der Startseite Ricardo ausserdem der Verweis zu sehen, dass Ricardo der grösste Online-Marktplatz der Schweiz ist. Der Verweis auf die Grösse könnte dem Skeptiker bereits als Vertrauensindikator dienen, denn die Grösse verweist implizit auf ein gewisses Alter sowie auf die Bekanntheit eines Online-Anbieters. Dieser Hinweis wird nicht als beeinflussende Werbung und somit als negativ wahrgenommen, sondern ist für ihn eine wichtige Information, die ihn bei seiner Entscheidung unterstützt.

Beim Angebot selbst ist wichtig, dass der Skeptiker schnell sieht, welche Auflagen oder welche Verbindlichkeiten er mit der Transaktion eingeht. Ihm ist wichtig, dass es gut erkennbar ist, welche Verpflichtungen er eingeht (V_77, 59.5 % „stark beachtet“ oder „beachtet“ (Anhang 7.6.2). Der Skeptiker surft immer mit einer latenten Angst, vom Anbieter übervorteilt zu werden und deshalb ist Angebotstransparenz für diesen Vertrauenstyp zentral.

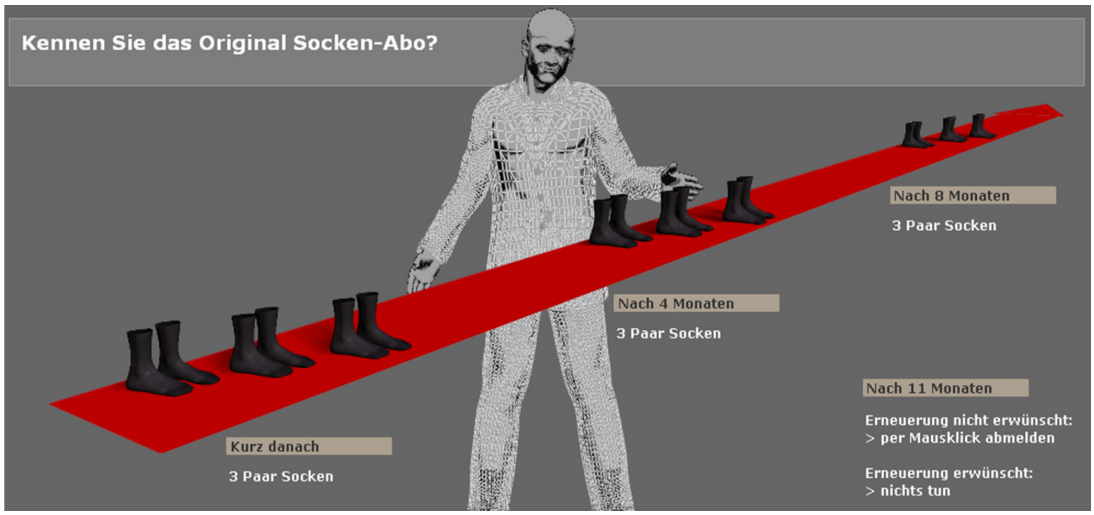


Abbildung 56: Nutzen und Verpflichtungen bei Blacksocks (Blacksocks, 2012)

Der Sockenlieferant Blacksocks zum Beispiel zeigt anhand eines Zeitstrahls grafisch auf (Abbildung 56), wann die Lieferungen erfolgen, wie viele Socken pro Lieferung eintreffen werden und dass man sich nach elf Monaten vom Abonnement abmelden muss, falls eine Erneuerung des Abonnements nicht erwünscht ist. Wird vom Nutzer nichts unternommen, verlängert sich das Abonnement automatisch. Detaillierte Informationen sind je nach Sockentyp und Lieferrhythmus erhältlich. Der Skeptiker achtet auf solche übersichtlichen Darstellungen seiner Rechte und Pflichten, er kann sich dadurch schneller orientieren und den Anbieter rasch einschätzen.

Interessant ist darüber hinaus, dass es für ihn nicht zentral ist, ob der Anbieter viele Informationen über das eigene Unternehmen anbietet (V_79, 20.6 % „wenig beachtet“ oder „nicht beachtet“, Anhang 7.6.2). Eigentlich wurde erwartet, dass der gut gebildete Skeptiker möglichst ausführlich über das Unternehmen informiert werden möchte, was jedoch nicht der Fall zu sein scheint.

Es kann angenommen werden, dass der Skeptiker viel Wert auf Unabhängigkeit legt und sich nicht gerne fremdbestimmen lässt. Dies könnte bedeuten, dass er auch im Netz nicht gerne einem vordefinierten Schema folgt, sondern lieber von Optionsmöglichkeiten profitiert. Demnach sollten Anbieter von Online-Geschäftsmodellen darauf achten, dem Skeptiker Wahlmöglichkeiten zur Verfügung zu stellen. Der Skeptiker will bei der Erstanmeldung entscheiden können, ob er sich nur temporär anmeldet oder ob er sich registrieren möchte. Der Bilderlieferdienst Posterjack zum Beispiel bietet den Nutzern zwei Möglichkeiten: registrieren und ein Kundenkonto einrichten oder direkt ohne Anmeldung bestellen, wie in Abbildung 57 dargestellt. Der Skeptiker wird sich bei einer Erstbestellung vermutlich nicht registrieren wollen, liest aber aufmerksam die aufgelisteten Vorteile im Falle einer nachträglichen Registrierung durch.

Abbildung 57: Wahlmöglichkeit zwischen Registrierung oder Direktbestellung bei Posterjack (Posterjack, 2012)

Es muss klar ersichtlich sein, weshalb welche Daten für einen Online-Service benötigt werden. Für den Skeptiker ist wichtig, dass der Anbieter nur Daten abfragt, die er auch tatsächlich benötigt, um seinen Dienst betreiben zu können (V_67, 46.8 % „stark beachtet“ oder „beachtet“, Anhang 7.6.2). Im Beispiel von Posterjack (Abbildung 57) ist nicht intuitiv klar, weshalb bei einer Posterbestellung die Telefonnummer angegeben werden muss. Deshalb ergibt es Sinn, wenn der Anbieter von sich aus darauf hinweist und erklärt, dass es sich nicht um ein Pflichtfeld handelt: „Sie können Ihre Telefonnummer hinterlassen, damit wir Sie in dringenden Fällen kontaktieren können.“ Dadurch können Unsicherheiten im Vorfeld eliminiert werden und der Skeptiker kann entscheiden, ob diese Erklärung die Datenpreisgabe rechtfertigt. Weiter ist darauf zu achten, dass möglichst wenige Pflichtfelder ausgefüllt werden müssen und dass die Angabe von Daten über das notwendige Minimum hinaus freiwillig ist (V_117, 43.4 % „stark beachtet“ oder „beachtet“, Anhang 7.6.4). Anbieter von Online-Geschäftsmodellen müssen beim Skeptiker darauf achten, dass nur diejenigen Daten als Pflichtfelder programmiert werden, welche für den Dienst effektiv benötigt werden.

Der Skeptiker weist zwar im Vergleich zu den anderen beiden Vertrauenstypen eine eher lockere Datenhandhabung auf.[44] Trotzdem ist ihm wichtig, dass die Angabe von Daten über das notwendige Minimum hinaus freiwillig ist.

Abbildung 58: Registrierung mit wenigen Pflichtfeldern bei Cineman (Cineman, 2012)

Die Community- und Informationsplattform für Film und Kino Cineman zum Beispiel verlangt für die Aktivierung des Accounts nur einen realen oder fiktiven Benutzernamen sowie eine gültige E-Mail-Adresse, wie in Abbildung 58 zu sehen ist. Alle weiteren Angaben basieren auf Freiwilligkeit. Zudem kann der Nutzer bereits bei der Registrierung entscheiden, für wen welche seiner Daten sichtbar sein sollen (Cineman, 2012). Diese auf Freiwilligkeit basierende Registrierung zeigt dem Skeptiker, dass der Anbieter die Bedürfnisse des Nutzers kennt und ernst nimmt.

Wichtig ist dem Skeptiker auch, dass der Anbieter unterschiedliche Möglichkeiten zur Kontaktaufnahme zur Verfügung stellt (V_180, 38.3 % „stark beachtet“ oder „beachtet“, Anhang 7.6.5). Bei der Beschreibung der Typen wurde angenommen, dass der Skeptiker eher Mühe hat, mit Menschen real in Kontakt zu treten und dass er diese lieber schriftlich online pflegt. Es könnte sein, dass der Skeptiker zur Sicherheit immer alles schriftlich regeln möchte. Er möchte kein Risiko eingehen und auch später noch auf die erhaltene Information zurückgreifen können. Der Online-Versandhändler für Schuhe und Mode Zalando zum Beispiel lässt dem Skeptiker den Freiraum, den er benötigt (Abbildung 59): Er hat unterschiedliche Optionen

[44] Zum Beispiel bewerteten 72.7 % das Item „Der Anbieter teilt mir mit, auf welche Art er meine Daten auswertet/analysiert.“ oder 65.8 % beim Item „Der Anbieter ermöglicht mir, selbst auszuwählen, an wen meine Daten weitergegeben werden.“ als „neutral“ bis „nicht beachtet“.

(Hotline, Telefax, E-Mail, Postweg), dieses Unternehmen zu kontaktieren, und auf der Seite ist ersichtlich, dass er bereits gekaufte Produkte nach bis zu 30 Tagen auf dem Postweg kommentarlos und kostenlos zurücksenden kann. Darüber hinaus wird mehrmals prominent auf die kostenlose Hotline und deren Belegzeiten verwiesen. Weiter hat der Skeptiker die Möglichkeit, Zalando über das soziale Netzwerk Facebook, über das Internet-Videoportal YouTube oder über den firmeneigenen Blog zu kontaktieren.

Abbildung 59: Kontaktmöglichkeiten bei Zalando (Zalando, 2012)

Interessant ist wiederum, dass für den Skeptiker nicht besonders wichtig ist, dass der Kundendienst einfach zu erreichen ist (V_114, 27.5 % „wenig beachtet“ oder „nicht beachtet“). Dieser Vertrauenstyp braucht verschiedene Optionen zur Kontaktaufnahme, das Unternehmen muss aber nicht rund um die Uhr mit voller Belegschaft erreichbar sein und Wartezeiten scheinen ihn nicht sonderlich zu stören.

Wie bereits bei der ersten Forschungsfrage ausgeführt, verlässt sich der Skeptiker nicht generell auf die Institution Internet, auf einen Anbieter oder, wie hier eruiert, auf einzelne Vertrauensfaktoren. Anbieter von Online-Geschäftsmodellen, welche den Skeptiker als Nutzer anvisieren, sollten tendenziell keine Angebote mit Abonnement-Verpflichtung anbieten. Ausserdem muss für ihn klar ersichtlich sein, welche Verpflichtungen er bei einem Anbieter eingeht. Dem Skeptiker ist es wichtig, dass der Anbieter schon eine Weile existiert und bekannt ist. Die Angabe von Daten, welche nicht intuitiv für den Dienst benötigt werden, sollte freiwillig sein. Weiter ist es von Vorteil, wenn dem Skeptiker die Möglichkeit eingeräumt wird, ohne Erklärungen vom Vertrag zurückzutreten. Der Skeptiker möchte möglichst unabhängig sein und deshalb muss man ihm einen grossen Handlungsspielraum geben.

4.2.2 Relevante Vertrauensfaktoren für den Praktiker (Vertrauenstyp 2)

Dieses Kapitel diskutiert die im Methodik-Kapitel 3.2.1 identifizierten relevanten Vertrauensfaktoren für den Praktiker (Vertrauenstyp 2). Dieser Vertrauenstyp achtet im Vergleich am stärksten auf alle vier Vertrauensfaktoren, wie in Abbildung 60 grafisch dargestellt ist.

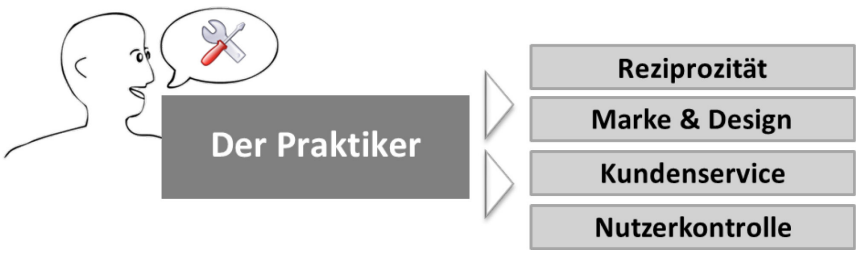


Abbildung 60: Relevante Vertrauensfaktoren für den Praktiker (Vertrauenstyp 2) (eigene Darstellung)

Gemäss dem Mittelwertvergleich im Methodenkapitel Tabelle 16 (Seite 138) ist für den Praktiker besonders die Reziprozität (Ø -.297) relevant, dicht gefolgt von Marke und Design (Ø -.258), danach folgen für ihn der Kundenservice (Ø -.227) sowie die Nutzerkontrolle (Ø -.084).

Da der Praktiker das Internet als Werkzeug und als Mittel zum Zweck betrachtet, schaut er sich sein Werkzeug – und somit die Vertrauensfaktoren – ganz genau an. Er ist es gewohnt, eine Bedienungsanleitung zur Hand zu nehmen und liest im Internet die zur Verfügung gestellten Informationen aufmerksam durch. Der Praktiker ist zwar im Umgang mit dem Internet geübt und hat Freude an der Technik, er könnte jedoch manchmal Mühe damit haben, Unwichtiges von Wichtigem zu unterscheiden. Da er gerne viel Zeit im Internet verbringt, möchte er auf Nummer sicher gehen und achtet vielleicht deshalb auf alle Vertrauensindikatoren. Der Praktiker kann es sich jedoch auch leisten, alles im Griff haben zu wollen, er hat Zeit, Freude am Vergleichen und er hat die Fähigkeiten dazu. Der Praktiker hat eine grosse Lebenserfahrung und achtet sehr genau auf die Qualität, er ist preisbewusst und könnte sogar als pingelig bezeichnet werden. Dass der Praktiker auf alle Vertrauensfaktoren achtet, könnte auch mit seiner Angst vor Verletzungen erklärt werden: Er möchte potenziellen Verletzungen ausweichen und achtet deshalb auf alles. Im Folgenden werden die Faktoren im Detail betrachtet und diskutiert, wie Online-Anbieter den Praktiker am besten ansprechen und was sie vermeiden sollten.

Reziprozität: Alle Items des Faktors Reziprozität sind für den Praktiker relevant, denn alle weisen einen Mittelwert kleiner 2.5 auf (Abbildung 61 & Anhang 7.6.1).

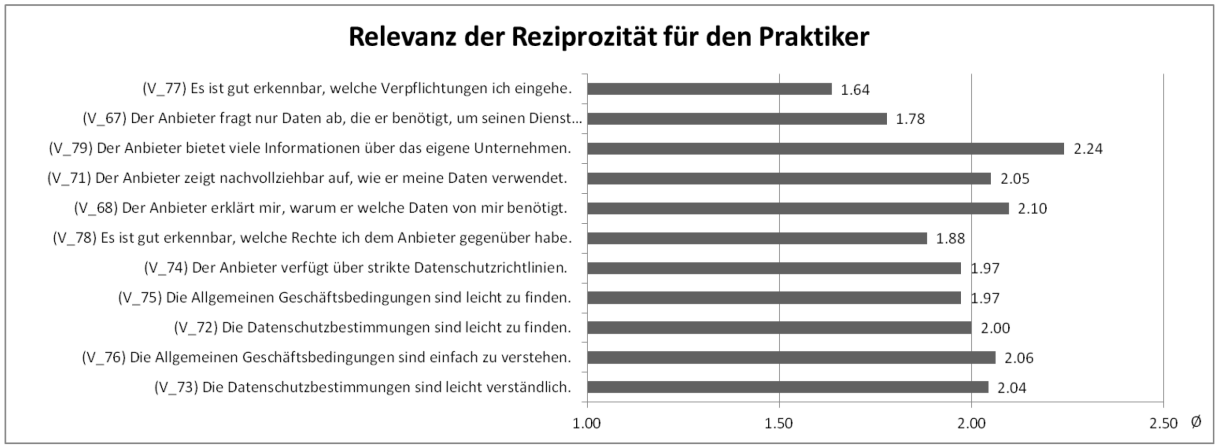


Abbildung 61: Mittelwerte der Items des Faktors Reziprozität des Praktikers (Interpretation: 1 „trifft zu"; 5 „trifft nicht zu")

Der Praktiker hat eine grosse Lebenserfahrung, nutzt das Internet im Vergleich am intensivsten und ist geübt im Umgang mit dem Netz (Kapitel 4.1.2.2). Da er tendenziell ein sparsamer Typ ist, verbringt er im Internet viel Zeit mit Vergleichen und sucht sich das für ihn optimale Angebot heraus. Während seiner Internetkarriere hat er schon einige unseriöse Anbieter erlebt und deshalb möchte er genau wissen, welche Verpflichtungen er als Nutzer eines Angebots eingeht und welche Gegenleistung er dafür bekommt (V_77, Ø 1.64, Abbildung 61). Wie viel kostet die Nutzung des Angebots? Gehe ich damit ein Abonnement mit wiederkehrenden Kosten ein oder ist die Nutzung gratis, werden dafür meine Daten kommerziell genutzt?

Im Allgemeinen fällt auf, dass Datenschutz für den Praktiker ein zentrales Anliegen ist. Der Praktiker achtet darauf, dass der Anbieter über strikte Datenschutzrichtlinien verfügt (V_74, Ø 1.97), dass die AGBs sowie die Datenschutzbestimmungen leicht zu finden sind (V_72, Ø 2.00; V_75, Ø 1.97), aber auch, dass diese auch verständlich formuliert sind (V_73, Ø 2.04; V_76, Ø 2.06). Dieser im Vergleich geübte Internetgänger liest demnach die Datenschutzrichtlinien und kann beurteilen, ob es sich um konsequente oder um eher lockere Richtlinien handelt. Für den Praktiker muss genau ersichtlich sein, welche Rechte er gegenüber dem Anbieter hat, dazu gehören insbesondere Informationen über Garantien, Rückgaberechte oder Lieferkonditionen (V_78, Ø 1.88). Der Praktiker will wissen, welche Daten zu welchem Zweck vom Anbieter gespeichert werden (V_68, Ø 2.10) und wie diese Daten weiterverwendet werden (V_71, Ø 2.05). Er ist der Meinung, dass der Anbieter nur jene Daten

abfragen sollte, die er für seinen Dienst auch benötigt (V_67, Ø 1.78), und er sieht sich in der Lage einzuschätzen, für welchen Dienst welche Daten benötigt werden. Will der Anbieter zusätzliche Daten erheben, muss er dies nachvollziehbar begründen, ansonsten bricht der Praktiker die Transaktion mit grosser Wahrscheinlichkeit ab. Dies ist insbesondere für Online-Geschäftsmodelle relevant, welche mit besonders sensiblen Kundendaten agieren. Bei Versandapotheken zum Beispiel können mit der Zeit Dossiers mit sensiblen Krankheitsbildern entstehen oder es können sich Hinweise zu einem möglichen Medikamentenmissbrauch kumulieren.

Abbildung 62: Visualisierung zur Sicherheit und Datenschutz bei Mycare (Mycare, 2012)

Ein Interessantes Beispiel ist deshalb die Online-Versandapotheke Mycare, welche explizit darauf hinweist, dass die persönlichen Daten ihrer Kunden einen ganz besonderen Schutz geniessen (Abbildung 62). Die Datenschutzbestimmungen und die AGBs sind in der Fusszeile der Seite einfach zu finden. Werden die Datenschutzbestimmungen von Mycare im Detail betrachtet, fällt dem Praktiker jedoch schnell auf, dass dieser „ganz besondere Schutz" gar nicht so umfassend ist: „Ihre persönlichen Daten werden von uns nur für die Bestell- und Zahlungsabwicklung benötigt und in diesem Rahmen gespeichert." Konkretere Informationen über die Art und Dauer der Datenspeicherung sind jedoch keine zu finden. Dafür aber Folgendes: „Aus Gründen der Sicherheit und zur Durchführung unseres pharmazeutischen Services erheben und speichern wir weitere Daten von Ihnen (…)." Was das Unternehmen unter „weitere Daten" versteht, wird nicht weiter ausgeführt. Die Versandapotheke hält des Weiteren fest: „Informationen zu Ihrer Medikation und zu Ihrem Gesundheitszustand werden nicht an Dritte weitergegeben." Wie diese Daten jedoch intern weiterverwendet werden, wird nicht erwähnt. Unter den Datenschutzbestimmungen wird der Nutzer darüber informiert, dass die Seite die Bewegungen ihrer Nutzer über Google Analytics anhand von Cookies analysiert und auswertet, wie diese Daten jedoch genau verwendet und gesichert werden, erwähnt der Anbieter nicht. Diese lückenhaften Informationen zum Datenschutz, insbesondere bei der Handhabung von Krankheitsdaten, genügen dem Praktiker nicht.

Neben ausführlichen Informationen über den Schutz der Daten erwartet der Praktiker auch Angaben über den Online-Anbieter. Für den Praktiker muss klar ersichtlich sein, mit welchem Unternehmen er seine Geschäfte tätigt, und er erwartet vom Anbieter detaillierte Informationen, damit er das Unternehmen einschätzen kann. Er sucht sich ganz spezifisch Informationen, um die Vertrauenswürdigkeit des jeweiligen Anbieters einstufen zu können. Er schätzt es demnach, wenn der Anbieter Informationen über das eigene Unternehmen zur Verfügung stellt (V_79, Ø 2.24, Abbildung 61). Der Suchmaschinenanbieter Google zum Beispiel bietet dem Praktiker auf der Startseite unter dem Link „Über Google" alle relevanten Informationen über das Unternehmen an. Auf dieser Informationsseite hat Google auf farbenfrohes und verspieltes Design verzichtet, die Seite ist hier äusserst schlicht in Grau- und Blau-Tönen gehalten und mit vielen übersichtlichen Textbausteinen und Links versehen.

Abbildung 63: Ausführliche Informationen bei Google (Google, 2012)

Wie in Abbildung 63 zu sehen ist, wird die Seite von einem Text über das Ziel von Google und eine kurze Beschreibung der Entstehungsgeschichte dominiert. Auf der linken Seite, unter der Rubrik „Überblick" findet der Praktiker ausführliche Informationen zu den verwendeten Technologien, den Geschäftsaktivitäten und der Philosophie von Google. Auf der rechten Seite wird Google „Auf einen Blick" zusammengefasst und die wichtigsten Links sind unter „Hilfreiche Links" gut gekennzeichnet. Google stellt dem Praktiker viele nützliche Informationen übersichtlich und nüchtern zur Verfügung.

Marke und Design: Der Praktiker achtet auf die Marke und das Design eines Anbieters, alle Items dieses Faktors sind für ihn relevant und weisen einen Mittelwert kleiner 2.5 auf (Abbildung 64 & Anhang 7.6.1).

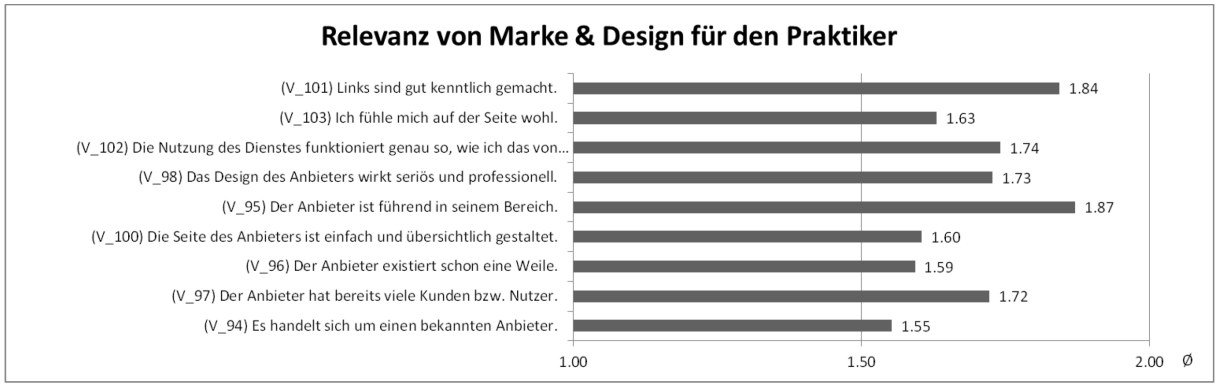


Abbildung 64: Mittelwerte der Items des Faktors Marke und Design des Praktikers (Interpretation: 1 „trifft zu"; 5 „trifft nicht zu")

Der Praktiker ist ein ressourcenbewusster Internetnutzer, welcher gerne Angebote im Netz vergleicht und das für ihn optimale Angebot sucht. Dabei achtet er insbesondere auf Hinweise, um die Marktstellung des Anbieters abschätzen zu können. Für den Praktiker ist die Bekanntheit ein Indiz dafür, dass es sich um einen seriösen, vertrauenswürdigen, qualitativ hochstehenden Anbieter handelt (V_94, Ø 1.55). Ein weiterer Nachweis der Vertrauenswürdigkeit ist für ihn die Anzahl der Jahre, die der Anbieter bereits im Geschäft ist (V_96, Ø 1.59). Bekannte Anbieter haben sich über einen längeren Zeitraum eine Reputation aufgebaut und haben deshalb auch viel zu verlieren. Ein weiter Hinweis auf die Bekanntheit eines Anbieters ist für den Praktiker der Kundenstamm (V_97, Ø 1.72). Je länger er existiert und je mehr Nutzer ein Dienst hat, desto besser und vertrauenswürdiger ist dieser. Wenn ein Anbieter führend in seinem Bereich ist (V_95, Ø 1.87), deutet das darauf hin, dass die versprochenen Leistungen auch tatsächlich erfüllt werden, anfängliche Probleme gelöst wurden und Abläufe und Services einwandfrei funktionieren. Ausserdem weiss der Praktiker aufgrund seiner Berufserfahrung, dass grosse Unternehmen auch grosse Mengen einkaufen können und im Prinzip die Produkte zu einem tieferen Preis verkaufen können.

Dass der Anbieter gut vernetzt ist, bereits eine Weile existiert und eine gewisse Grösse aufweist, erkennt der Praktiker unter anderem an einer hohen Listung bei Suchmaschinen. Der Praktiker weiss, wie Rankings bei Suchmaschinen funktionieren: Je beliebter und je verlinkter eine Seite ist, desto schneller taucht sie weit oben in der Resultatliste auf (Sen, 2005). Hohe Rankings in Suchmaschinen weisen für den

Praktiker auf weite Verbreitung hin und generieren dadurch Vertrauen. Suchmaschinenoptimierung bedeutet demnach, ein Online-Angebot durch Marketingmassnahmen optimal zu vernetzen. Bei der Suchmaschinenoptimierung ist jedoch wichtig, dass die ethischen Richtlinien eingehalten werden und auf Spamming[45], Brückenseiten[46] oder Linkfarms[47] verzichtet wird. Es erstaunt nicht, dass einige Unternehmen versuchen, die Rankings und Bewertungen zu ihren Gunsten zu beeinflussen oder Empfehlungen anzukurbeln. DeinDeal zum Beispiel gibt für eine erfolgreiche Weiterempfehlung ihres Dienstes pro Kundenanwerbung CHF 30.-- aus.

Gewisse Anbieter gehen sogar so weit, Kundenrezensionen zu manipulieren. Aggressive Werbung und das Ankurbeln von Word-of-Mouth[48] werden im Allgemeinen zwar toleriert, eine absichtliche Täuschung der Nutzer ist jedoch inakzeptabel. Blogger machen sich einen Spass daraus, die IP-Adressen von auffällig positiven „Kundenrezensionen" zurückzuverfolgen. Steht hinter dem vermeintlichen Nutzer der Online-Anbieter selbst oder eine PR-Agentur, kann es schnell zum „David gegen Goliath"-Effekt[49] kommen, mit unabsehbaren Reputationsschäden für die Marke und das Unternehmen. Manipulatives Kommentieren kann enorm weite Kreise ziehen und einen direkten Einfluss auf den Handlungsspielraum eines Unternehmens haben.

Der Praktiker weiss, dass Werbung in Printmedien, TV, Radio oder auf Plakaten sehr teuer sein kann. Ihm fällt deshalb sofort auf, wenn junge Online-Anbieter in der realen Welt für ihre Marke oder ihr Produkt werben. Hat der Anbieter durch ein In-

---

[45] Unter Spamming werden alle Suchmaschinenmanipulationen subsumiert, welche eine Website unter einem Stichwort listen, ohne dass sich die Seite mit dem jeweiligen Thema beschäftigt (Alby & Karzauninkat, 2007).

[46] Brückenseiten (Doorway Pages) fungieren als Zwischenseiten und verweisen automatisch auf die eigentliche Webpräsenz (Winkler, 2007; Alby & Karzauninkat, 2007).

[47] Linkfarms sind grosse Ansammlungen von Seiten im Web, die nur dazu dienen, möglichst viele Links auf die eigentliche Webpräsenz zu legen und damit die Suchmaschinen zu manipulieren (Alby & Karzauninkat, 2007).

[48] Kimmel (2010) definiert Word-of-Mouth als die positive oder negative Kommunikation zwischen zwei oder mehreren Personen über eine Marke, ein Produkt oder einen Service. Er betont, dass der Empfänger davon ausgeht, dass der Mitteilende keine kommerziellen Interessen im Hinblick auf den Informationsaustausch verfolgt, und diesen deshalb als besonders glaubwürdig ansieht.

[49] Als „David gegen Goliath"-Effekt werden Solidaritätsbekundungen durch Verlinkung und Vernetzung unter Bloggern und Internetnutzern gegen Konzerne und Marken bezeichnet.

serat sein Interesse geweckt, informiert er sich online näher über das Angebot. Am wichtigsten aber ist, dass er die Marke bereits einmal gesehen und registriert hat. Diesen Wiedererkennungseffekt beim Praktiker sollten insbesondere junge Start-up-Unternehmen ausnützen, welche noch nicht breit bekannt sind. Besonders bei innovativen Plattformen berichten Zeitungen oder Radiostationen gerne von sich aus über das Neueste im Netz und die Anbieter bekommen kostenlose Publicity. Der Schweizer Radiosender DRS 2 zum Beispiel besprach in seiner Sendung „Reflexe" die Möglichkeiten des Crowdfunding (DRS 2, 2012). Diese Schwarmfinanzierung beruht darauf, dass Geldsuchende ihre Projekte und Ideen vorstellen und erklären, wie viel Geld sie dafür benötigen. Das Publikum entscheidet, wie viel es wem spenden will. Das Prinzip dabei ist, dass viele Personen mit kleinen Geldbeträgen gemeinsam Grosses bewirken können.

Abbildung 65: Diskussion über Crowdfunding auf DRS 2 (DRS 2, 2012; Wemakeit, 2012; 100Days, 2012)

Die ersten Schweizer Crowdfunding-Plattformen sind wemakeit.ch und 100-days.net (Abbildung 65). Die innovative Geschäftsidee und die beiden Plattformen wurden von Spezialisten in der Sendung durchleuchtet und diskutiert und die Gründer beider Plattformen wurden interviewt. Durch die Besprechung bei „Reflexe" haben beide Unternehmen an Publizität gewonnen. Der Praktiker sagt von sich selbst, dass er sich für neue Entwicklungen im Internet interessiert (V_43, 67.7 % „trifft zu" oder „trifft eher zu") und dass er gerne neue Online-Plattformen und Applikationen ausprobiert (V_44, 40.3 % „trifft zu" oder „trifft eher zu"). Hat der Praktiker die Sendung „Reflexe" auf DRS 2 gehört, informiert er sich mit grosser Wahrscheinlichkeit detaillierter über diese beiden Firmen und die Möglichkeiten des Crowdfunding.

Das Design einer Homepage ist speziell für erfahrene Nutzer ein wichtiges Indiz für oder gegen eine Transaktionsentscheidung. Der Praktiker scheint die For-

schungsergebnisse von Riegelsberger und Sasse (2001) zu bestätigen: Er ist viel und oft im Internet und erkennt bereits anhand des Designs, ob er einem Anbieter vertrauen kann oder nicht. Eine Seite sollte seriös und professionell gestaltet sein (V_98, Ø 1.73), damit sich der Praktiker auch wohlfühlt (V_103, Ø 1.63). Sie muss einfach und übersichtlich (V_100, Ø 1.60) daherkommen und die relevanten Links sollten gut kenntlich gemacht sein (V_101, Ø 1.84). Wichtig zu wissen ist, dass Nutzer je nach Online-Geschäftsmodell gewisse logische Abfolgen oder Schemata erwarten, die sie bereits von anderen Anbietern kennen (V_102, Ø 1.74). Dieses Zurückgreifen auf bereits Erlerntes verringert den kognitiven Aufwand der Nutzer und erleichtert den Umgang mit neuen Anbietern.

Abbildung 66: Terminfindung leicht gemacht bei Doodle (Doodle, 2012)

Die Startseite des Terminfindungsanbieters Doodle zum Beispiel ist sehr übersichtlich, reduziert und einfach gestaltet, wie in Abbildung 66 zu sehen ist. Auf den ersten Blick ist erkennbar, dass die Kernkompetenz dieses Anbieters die Terminfindung ist: Der Slogan „Terminfindung leicht gemacht“, der Button „Einen Termin finden“, aber auch die verwendeten typischen Kalender-Symbole sind eindeutige Hinweise. Ausserdem ist auf der Startseite des Anbieters der Prozess einer Terminfindung einfach in drei Schritten dargestellt. Genau wie im realen Leben auch müssen mögliche Termine eruiert und eine Umfrage erstellt werden. Die Umfrage wird den Teilnehmern per Link, zum Beispiel per E-Mail, zugestellt und gemeinsam wird ein Termin festgelegt. Dieser Prozess ergibt für den Praktiker intuitiv Sinn und er fühlt sich auf der Seite wohl.

Kundenservice: Alle untersuchten Items weisen einen Mittelwert auf, welcher unter 2.5 liegt (Abbildung 67 & Anhang 7.6.1). Somit sind für den Praktiker alle Items des Faktors Kundenservice relevant.

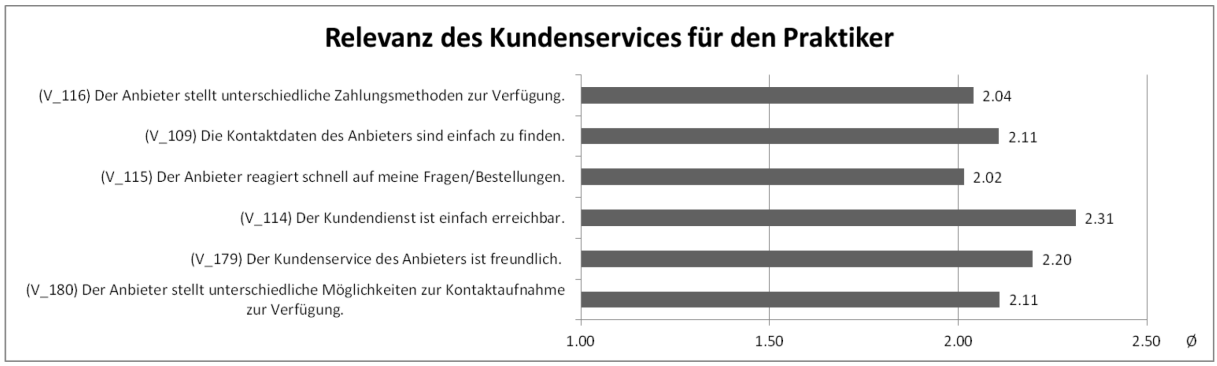


Abbildung 67: Mittelwerte der Items des Faktors Kundenservice des Praktikers (Interpretation: 1 „trifft zu“, 5 „trifft nicht zu“)

Der Praktiker hat sein Leben lang hart gearbeitet und viele Erfahrungen sammeln können. Er achtet sehr genau auf die Angebotsqualität und ist äusserst preisbewusst. Die versprochene und somit erwartete Leistung muss vom Online-Anbieter immer erfüllt werden. Ist dies nicht der Fall oder treten bei der Transaktion Fragen auf, wendet sich der Praktiker an den Kundenservice. Da der Praktiker viele Geschäfte im Internet tätigt, hat er immer wieder mit unterschiedlich professionellen Online-Anbietern zu tun und kann die Qualität des angebotenen Kundenservice schnell einschätzen und bewerten. Wie in Abbildung 67 zu sehen, ist dem Praktiker wichtig, dass der Kundenservice schnell, einfach und freundlich auf seine Anliegen reagiert (V_115, Ø 2.02; V_114, Ø 2.31; V_179, Ø 2.20).

Wichtig ist zudem, dass die Kontaktdaten des Anbieters auf der Seite einfach zu finden sind und dass unterschiedliche Möglichkeiten zur raschen Kontaktaufnahme bestehen (V_109, Ø 2.11; V_180, Ø 2.11). Dies können eine Customer-Hotline ohne endlose Warteschlaufen, E-Mail-Adressen oder Live-Chats mit den Mitarbeitern sein. Ausserdem sind Foren oder Communitys denkbar, in welchen Internet-Evangelisten[50] anderen Nutzern weiterhelfen und untereinander ihr Wissen austauschen. Kundenfreundlich ist für häufig gestellte Fragen auch der Verweis auf FAQ-Seiten. Die Erwartungshaltung der stetigen Erreichbarkeit ist besonders von kleinen und jungen Unternehmen schwer zu erfüllen, da nur wenige Mitarbeiter zur Verfügung stehen. Dies kann bei einer schriftlichen Anfrage zum Beispiel durch eine au-

[50] Internet-Evangelisten sind aktive Internetnutzer und sie gestalten das geschehen im Internet mit. Sie können durch eine offene, transparente und ehrliche Ansprache zu Customer-Evangelisten werden. Diese leisten einen wesentlichen Beitrag bei der Verbreitung von Botschaften und können das Image des Unternehmens positiv beeinflussen (Meckel, 2008a; Huber, 2008).

tomatisch generierte Bestätigungs-E-Mail entschärft werden, in der versprochen wird, baldmöglichst auf das Anliegen einzugehen. Der freundliche Umgangston ist für den Praktiker eine Selbstverständlichkeit. Er will als gleichberechtigter Partner wahrgenommen werden und auf gleicher Augenhöhe kommunizieren.

Vom Praktiker ist zu erwarten, dass er bei Fragen oder Unsicherheiten schnell auch ausserhalb der Anbieterseite nach einer Lösung sucht. Zum Beispiel hält er nach Antworten auf seine Fragen auf YouTube Ausschau oder sucht über Suchmaschinen nach Fachforen und Chats, die ihm weiterhelfen können. Online-Anbieter müssen demnach ihre Kunden nicht nur über ihre eigene Seite betreuen, sondern sich in den Kunden hineinversetzen und dort Informationen anbieten, wo der Praktiker danach sucht. Verlinkungen, zum Beispiel von YouTube-Videos, sind von Praktikern gern gesehen. Nielsen (1999) formuliert dies folgendermassen: "Connected to the rest of the Web with links in and out. Not being afraid to link to other sites is a sign of confidence, and third-party sites are much more credible than anything you can say yourself. Isolated sites feel like they have something to hide." Dabei spielt es eine untergeordnete Rolle, ob die Beiträge vom Unternehmen oder von den Nutzern kreiert wurden, in erster Linie ist es wichtig, dass der Beitrag weiterhilft. Das Unternehmen tut aus Transparenzgründen gut daran, sich immer als Absender einer Botschaft zu identifizieren.

Was passieren kann, wenn Anbieter die Anliegen seiner Kunden nicht ernst nehmen, verdeutlicht der Dell-Hell-Case[51]. Ein einzelner Blogger kritisierte den mangelnden Kundenservice und entfachte so einen Sturm negativer Publicity, der die Reputation der Firma nachhaltig beeinträchtigte. Ein gut funktionierender Kundenservice ist für Unternehmen im Netz elementar. Insbesondere der Praktiker wartet nicht lange, bis er seine Erfahrungen mit seiner Community teilt. Der Anbieter sollte

[51] Der unzufriedene Dell-Kunde Jeff Jarvis schrieb im Juni 2005 seine Erlebnisse auf seinem Blog BuzzMachine.com nieder und erreichte damit unzählige Gleichgesinnte. Sein Blog wurde zur Kommunikationsplattform für verärgerte Dell-Kunden und innerhalb kurzer Zeit wurde „Dell Hell" zum Begriff (Jarvis, ab Juni 2005). Jeff wurde zum Sprecher der Dell-Hell-Community und 37 Prozent aller Verlinkungen der Informationsströme wurden von BuzzMachine dominiert (Meckel, 2008b). Laut BusinessWeek wurde seine Seite täglich 10'000-mal aufgerufen (Lee, 2005). Unkoordinierte und ungenügende Reaktionen von Dell verschärften die Situation und die Firma musste ihr Kundenservice-Forum wegen Überlastung vom Netz nehmen. Heute hat Dell den Umgang mit seinen Kunden grundlegend restrukturiert, kommuniziert dialogorientiert mit den Kunden im Web 2.0 und ist führend im Bereich Online-Kundenservice.

vom Wissen des Praktikers profitieren und die Sozialen Medien bieten zahlreiche Möglichkeiten, um mit den Kunden in Kontakt zu treten und den Dialog mit ihnen zu pflegen. Das Online-Engagement von Kunden kann auch zur Produktverbesserung und Angebotserweiterung genutzt werden. Zum Beispiel könnte eine Ideenbox lanciert werden, auf der Änderungswünsche und Verbesserungsvorschläge eingereicht und von den Nutzern gleich bewertet werden können. Die vom Anbieter umgesetzten Ideen könnten prämiert oder ausgezeichnet werden.

Starbucks zum Beispiel hat die Website „My Starbucks Idea“ (Abbildung 68) aufgeschaltet und gibt damit den Konsumenten die Möglichkeit, ihre Bedürfnisse, Wünsche oder Ideen auf der Plattform offen zu kommunizieren. Tausende Nutzer, Konsumenten und Mitarbeiter veröffentlichten Ideen, wie zum Beispiel die Qualität des Kaffees verbessert werden könnte oder welche neuen Produkte eingeführt werden könnten. Eine solche Ideenbox gibt dem Unternehmen die Möglichkeit, die Kundenbedürfnisse besser zu verstehen und diese aktiv in den Verbesserungsprozess einzubeziehen. Zudem ermöglicht es eine solche Plattform, dass Kundenbeschwerden nicht auf einem für das Unternehmen unbekannten Blog diskutiert, sondern direkt ans Unternehmen herangetragen werden. Der Praktiker fühlt sich dadurch ernst genommen und integriert.

Abbildung 68: Kundenintegration bei Starbucks (Starbucks, 2012)

Der Praktiker nutzt zum Beispiel auffallend oft den Microbloggingdienst Twitter (zu 9.8 % mindestens „einmal pro Woche“, Anhang 7.5.7). Deshalb macht es Sinn einen Twitter-Account einzurichten, um den Praktiker einzubinden. Das deutsche Telekommunikationsunternehmen Telekom zum Beispiel bietet ihren hilfesuchenden Kunden seit Mai 2010 zusätzlich einen Service über Twitter an (Abbildung 69). Sieben Mitarbeiter stehen den Kunden zu den klassischen Öffnungszeiten (8.00 bis 20.00

Uhr) unter www.twitter.com/telekom_hilft für Fragen zur Verfügung: „Hier hilft das Telekom Service-Team in der festen Überzeugung, dass Service mit 140 Zeichen geht.“ (Telekom, 2012). Der Vorteil für den Praktiker von Twitter gegenüber dem telefonischen Kundenservice ist eindeutig das Fehlen der Warteschleife. Es wird nicht erwartet, dass per Twitter schneller eine Antwort eintrifft als per Telefon, sondern dass die manchmal halbstündige Wartezeit produktiv genutzt werden kann. Ein weiterer Vorteil ist, dass man nicht etliche Male weiterverbunden wird und das Problem nur einmal geschildert werden muss. Der Anbieter hat den Vorteil, dass der Nutzer das Problem auf den Punkt bringen muss, was Zeit und Kosten spart.

Abbildung 69: Kundenservice über Twitter bei der Telekom (Telekom, 2012)

Des Weiteren achtet der Praktiker darauf, ob verschiedene Zahlungsmethoden zur Verfügung stehen (V_116, Ø 2.04). Dies gibt dem Praktiker einen Hinweis darauf, ob der Anbieter technisch versiert ist und auf die unterschiedlichen Bedürfnisse der Kunden eingeht. Beim nächsten Faktor Nutzerkontrolle wird diskutiert, dass der Praktiker nicht unüberlegt seine Daten zur Verfügung stellt. Optionen bei der Zahlungsmethode ermöglichen es ihm zu entscheiden, ob er zum Beispiel seine Kreditkartendaten bei diesem Anbieter angeben möchte oder nicht. Kennt er einen Anbieter schon lange, hat er diese im Profil hinterlegt, ist er aber noch unsicher, möchte er lieber per Vorkasse mit Banküberweisung oder mit PayPal bezahlen. Traut er einem Anbieter anfänglich gar nicht, hält ihn die Option, auf Rechnung bezahlen zu können, vom Wechsel zu einem anderen Anbieter ab.

Nutzerkontrolle: Alle Items des Faktors Nutzerkontrolle sind für den Praktiker relevant, alle weisen einen Mittelwert kleiner 2.5 auf (Abbildung 70 & Anhang 7.6.1).

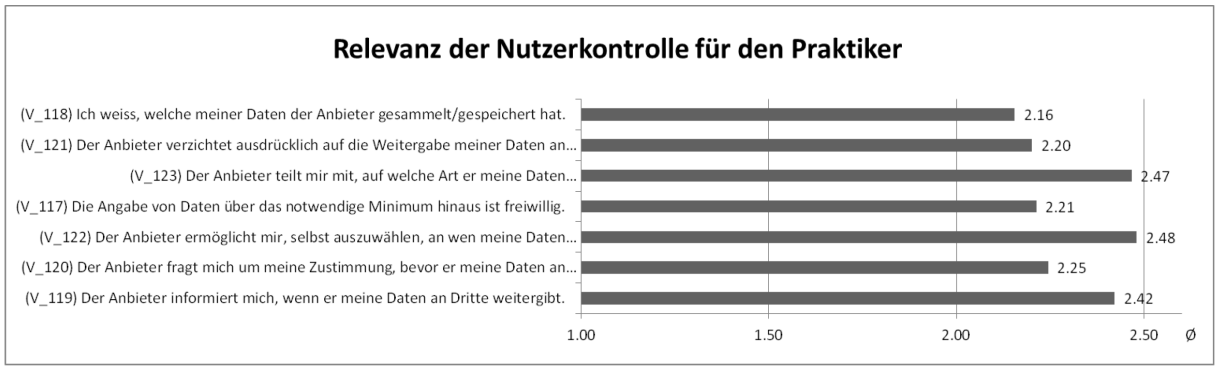


Abbildung 70: Mittelwerte der Items des Faktors Nutzerkontrolle des Praktikers (Interpretation: 1 „trifft zu“, 5 „trifft nicht zu“)

Dem Praktiker ist es ein wichtiges Anliegen, dass die Kontrolle über die persönlichen Daten bei ihm als Nutzer liegt, auch wenn diese auf der Applikation des Anbieters zur Verfügung gestellt werden. Die Kontrolle fängt damit an, dass der Nutzer bereits bei der Anmeldung auf der Seite selber entscheiden kann, welche Daten er von sich zur Verfügung stellen will. Durch seine Erfahrung weiss er, welche Daten für welchen Dienst benötigt werden. Die Angabe von Daten über das notwendige Minimum hinaus muss also auf Freiwilligkeit beruhen (V_117, Ø 2.21), bei zu vielen Pflichtfeldern kann es sein, dass der Praktiker die Anmeldung abbricht.

Der Praktiker will, dass der Anbieter ihn als registrierten Nutzer proaktiv über den eigenen Gebrauch der Daten aufklärt (V_123, Ø 2.47). Auf der Seite, beispielsweise unter „Mein Profil“ erwartet er eine Stellungnahme des Anbieters über die Handhabung der persönlichen Daten und Informationen darüber, wie die Daten vom Anbieter gespeichert, ausgewertet und analysiert werden. Wie in Abbildung 70 ersichtlich, ist dem Praktiker besonders wichtig, dass er weiss, welche Daten der Anbieter gesammelt und gespeichert hat (V_118, Ø 2.16). Über ein Login-Verfahren könnten die eigenen Daten eingesehen, geändert oder gelöscht werden. Am besten wäre eine Verlinkung zu weiteren Informationen, wo aufgezeigt wird, welche Daten wie lange gespeichert werden, weshalb diese gespeichert werden, was damit geschieht, wie diese gesichert sind und welche Garantien diesbezüglich bestehen. Insbesondere in Netzwerken sind Angaben zur Sichtbarkeit des eigenen Profils und der Aktivitäten elementar. Ist mein Profil für alle einsehbar oder nur für Mitglieder? Werden meine Beiträge auf Walls oder in Gruppen über Suchmaschinen gefunden? Dies könnten Gründe dafür sein, weshalb der Praktiker im Vergleich nur selten auf sozialen Netzwerkseiten und Online-Communitys anzutreffen ist.

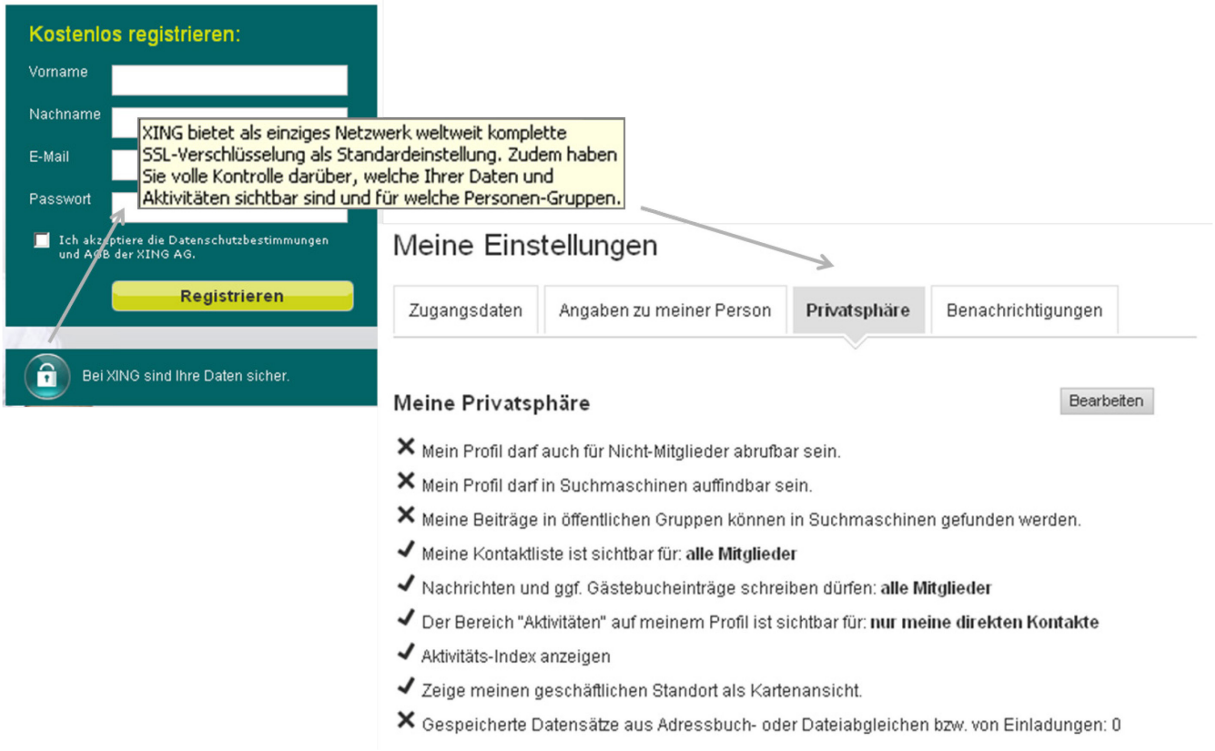


Abbildung 71: Kontrolle über die eigenen Daten bei Xing (Xing, 2012)

Das soziale Netzwerk Xing zum Beispiel macht den Nutzer bereits bei der Registrierung auf die Kontrollmöglichkeiten der eigenen Daten aufmerksam: „Bei Xing sind Ihre Daten sicher." (Abbildung 71). Im Profil unter „Meine Einstellungen" können die Privatsphäre-Einstellungen schnell und einfach bearbeitet und verwaltet werden.

Darüber hinaus muss auf der Seite ersichtlich sein, wie der Anbieter die Datenweitergabe an Dritte handhabt. Der Praktiker ist nicht der Meinung, dass durch die Eingabe der Daten die Verfügungsgewalt darüber vom Nutzer zum Anbieter übergehen; für ihn werden die persönlichen Daten nur für diesen einen Dienst ausgeliehen. Deshalb will er nicht, dass seine Daten ohne sein Wissen und seine Einwilligung an Dritte weitergegeben werden (V_121, Ø 2.20; V_120, Ø 2.25; V_119, Ø 2.42). Der Anbieter kann beim Praktiker Vertrauen generieren, indem er ausdrücklich auf die Weitergabe der Daten an Dritte verzichtet und dies auch auf der Seite, zum Beispiel bei der Anmeldung, kommuniziert. Wenn dieser Typ sich vom Dienst abmeldet, erwartet er höchstwahrscheinlich, dass seine Daten vollumfänglich gelöscht werden.

Abbildung 72: Auf den Praktiker zugeschnittene Registrierung bei eDarling (eDarling, 2012)

Bei der Auswertung der Vertrauenstypen haben wir gesehen, dass der Praktiker überdurchschnittlich oft Dating-Plattformen nutzt (Kapitel 4.1.2). In Abbildung 72 ist eine für den Praktiker fast optimale Einstiegsseite zur Registrierung bei einem Partnervermittlungsanbieter abgebildet. Auf den ersten Blick ist klar ersichtlich, um welchen Anbieter es sich handelt (Marke) und was dieser verspricht: „Partnervermittlung auf hohem Niveau“. Die Seite ist einfach und übersichtlich gestaltet (Design). Das Reziprozitätsverhältnis wird kurz und prägnant beschrieben mit: „Melden Sie sich kostenlos an & finden Sie den Partner, der wirklich zu Ihnen passt.“ Der Verweis auf die Handhabung der persönlichen Daten spricht den Faktor Nutzerkontrolle an: „Persönliche Daten werden absolut vertraulich behandelt“. Empfehlungen sind prominent vertreten: TÜV-Zertifikate oder Testsieger-Abzeichen von Computer Bild sind unübersehbar unter dem Registrier-Button platziert und bürgen für eine sichere und seriöse Partnersuche. Einzig der Faktor Kundenservice fehlt; für den Praktiker bedeutet es jedoch wenig Aufwand, über die Unterseite „Ratgeber“ Antworten auf seine Fragen zu erhalten oder Kontakt mit dem Anbieter aufzunehmen. Bei seiner Suche nach Kontaktdaten stösst er auf folgendes Pop-up: „Zufrieden? – erzählen Sie es Ihren Freunden! Unzufrieden? – erzählen Sie es uns!“ mit der Verlinkung zur Kontaktaufnahme. Spätestens jetzt hat der Praktiker erkannt, dass der Anbieter weiss, worum es geht.

4.2.3 Relevante Vertrauensfaktoren für den Sozialen (Vertrauenstyp 3)

Dieses Kapitel befasst sich mit den im Methodik-Kapitel 3.2.2 (Tabelle 16) identifizierten relevanten Vertrauensfaktoren für den Sozialen (Vertrauenstyp 3). Wie in Abbildung 73 zusammengefasst, achtet er insbesondere auf die Marke und das Design (Ø -.117), den Kundenservice (Ø -.086), sowie auf das Reziprozitätsverhältnis (Ø -.013). Für ihn ist hingegen die Nutzerkontrolle (Ø .027) im Vergleich zu den anderen Vertrauenstypen für die Vertrauensbildung weniger relevant.

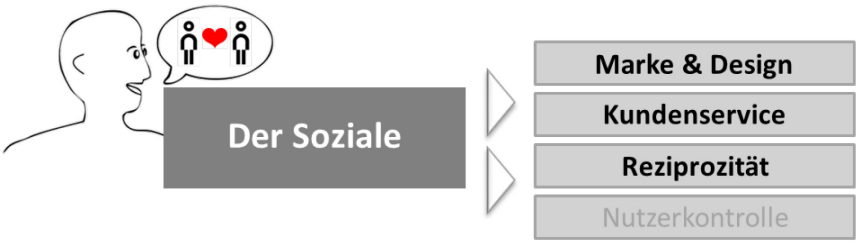


Abbildung 73: Relevante Vertrauensfaktoren für den Sozialen (Vertrauenstyp 3) (eigene Darstellung)

Dass der Faktor Nutzerkontrolle für den Sozialen weniger wichtig sein könnte, hat sich bereits bei der Analyse der Cluster abgezeichnet. Er tendiert zum Teamplayer und fällt Entscheide in der Gruppe. Somit fühlt er sich wohl, wenn er auch die Kontrolle gemeinsam mit anderen Menschen wahrnehmen kann. Deshalb achtet er im Vergleich auch im Online-Umfeld nicht stark darauf, wer die Gewalt über seine Daten hat und wie diese gehandhabt werden. Er ist nicht sonderlich oft im Internet anzutreffen und wenn, dann nicht auf Seiten, bei denen viele persönliche Daten abgefragt werden. In der bisherigen Analyse wurde angenommen, dass er bis jetzt keine negativen Erfahrungen mit Anbietern und deren Datenhandhabung gemacht hat und dass er kein offenes Ohr für Datenschutzskandale und Systempannen hat. Er liest und informiert sich, nimmt aber weniger an Konversationen teil und macht sich vielleicht deshalb über seine Datenhandhabung und die damit verbunden Risiken vergleichsweise wenige Gedanken. Es könnte aber auch sein, dass sich der Soziale mit Themen zum Datenschutz und der Datenhandhabung nicht auskennt und deshalb dem Faktor Nutzerkontrolle im Vergleich weniger Beachtung schenkt.

Marke und Design: Der Soziale achtet während einer Transaktion am stärksten auf den Faktor Marke und Design, um die Vertrauenswürdigkeit des Geschäftsmodell-Anbieters abschätzen zu können. Deshalb ergibt es Sinn, dass alle Items des Faktors Marke und Design einen Mittelwert kleiner als 2.5 aufweisen und für den Sozia-

len relevant sind (Abbildung 74 & Anhang 7.6.1). Er ist im Umgang mit dem Internet mässig geübt und als Kompensation für das niedrige Vertrauen in den Anbieter achtet er deshalb auf Indikatoren von aussen, um die Vertrauenswürdigkeit eines Anbieters einzuschätzen.

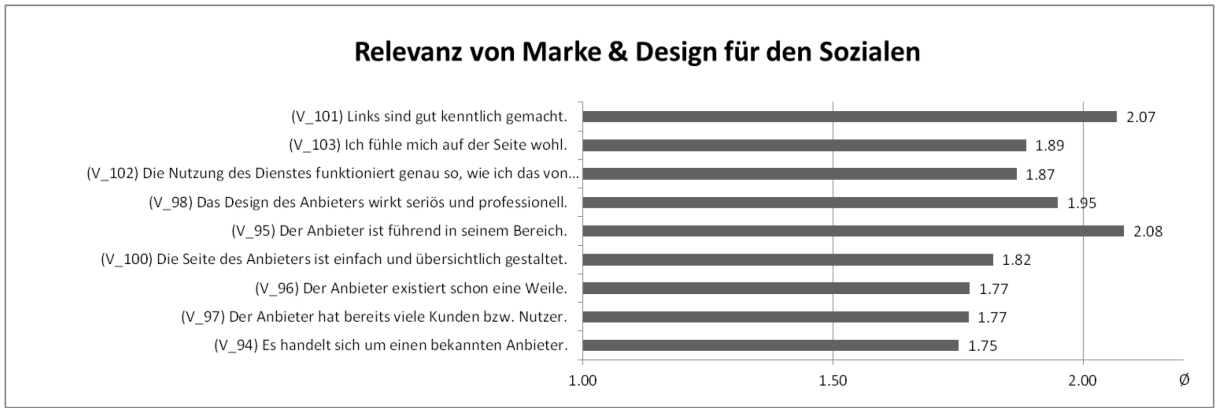


Abbildung 74: Mittelwerte der Items des Faktors Marke und Design des Sozialen (Interpretation: 1 „trifft zu“, 5 „trifft nicht zu“)

Der Soziale ist im Umgang mit dem Internet etwas unsicher, zögert oft und benutzt im Vergleich wenig unterschiedliche Online-Geschäftsmodelle. Er nutzt das Internet zwar seit vielen Jahren, jedoch nicht sehr intensiv (Anhang 7.5.7). Online-Anbieter müssen deshalb beim Sozialen Überzeugungsarbeit leisten. Starke Marken und ein klares Design helfen dabei massgeblich. Für den Sozialen ist es schwer, sich zwischen den vielen und international aktiven Anbietern zu entscheiden und seriöse Anbieter von unprofessionellen zu unterscheiden. Die Auswertungen haben gezeigt, dass der Soziale insbesondere bekannten, grossen Anbietern mit einem etablierten Kundenstamm vertraut, welche bereits eine Weile auf dem Markt existieren. Doch wie kann der Anbieter diese Attribute auf einer Hompage glaubhaft kommunizieren oder darstellen? Das wichtigste Item für den Sozialen ist die Bekanntheit des Anbieters (V_94, Ø 1.75). Eine hohe Bekanntheit könnte ein Anbieter zum Beispiel mit einem Verweis auf Rankings vermitteln. Google zum Beispiel war gemäss Interbrand-Ranking letztes Jahr auf dem vierten Platz der wertvollsten Marken der Welt 2011 (APA, 2012). Bei der Veröffentlichung einer solch guten Rankingposition könnte Google dies für den jeweiligen Tag in den Schriftzug einarbeiten und unter „Über Google“ dauerhaft aufführen.

Um einen Hinweis auf die eigene Marktmacht zu platzieren (V_95, Ø 2.08), könnten Online-Anbieter ihre Marken mit Slogans ergänzen: zum Beispiel „Marktführer in Deutschland“, „Der grösste Online-Händler der Schweiz“, „Führen-

des Reiseunternehmen“ oder „Die beliebteste Dating-Plattform“. Dies ist nur so lange möglich, wie die Bezeichnung auch zutrifft, und muss im Falle einer Änderung umgehend angepasst werden. Auch ein Vermerk über die Anzahl der getätigten Bestellungen ist denkbar: „Heutige Bestellsumme: 2,3 Millionen CHF“ oder „Über 1’000 Bestellungen am Tag“. Der Handelsmarktplatz eBay zum Beispiel nutzt seine Marktmacht als Verkaufsargument. Es steht zwar nicht prominent auf der Startseite von eBay, jedoch wird der Slogan „eine der grössten deutschen Shopping-Websites“ der Marke angehängt. Wie in Abbildung 75 aufgezeigt, erscheint der Slogan bei der Suchmaschine Google sowie im Register von Windows Explorer. Dieser Hinweis wirkt auf den Sozialen nicht etwa aufdringlich, sondern vertrauensbildend und kompetent.

Abbildung 75: Verweis auf die Marktmacht bei eBay (eBay, 2012)

Nicht nur Marktmacht und Grösse strahlen Sicherheit und Vertrauen aus, auch das Alter macht attraktiv (V_96, Ø 1.77). Beständigkeit ist in der sich schnell verändernden Welt des Internets auch für den Sozialen eine wichtige Eigenschaft. Deshalb könnten Online-Anbieter prominent auf ihr Gründungsjahr hinweisen, und dies bereits in der Marke, wie das Modehaus Cerruti mit seinem Parfüm „Cerruti 1981“, oder aber mit einem Hinweis „Since 1995“, „Gegründet 2001“ oder „seit 10 Jahren kompetent“.

Abbildung 76: Verweis auf die Anzahl Nutzer des Studienwahl-Navigators (HAW-Hamburg, 2012)

In der vorhergehenden Analyse wurde festgestellt, dass der Soziale bei der Nutzung von Plattformen eher zurückhaltend ist und er sich erst registriert, wenn er weiss, dass viele Personen das Angebot nutzen. Deshalb ist für ihn das Wissen über die Anzahl der Nutzer relevant (V_97, Ø 1.77). Die Hochschule für Angewandte Wissenschaften Hamburg zum Beispiel macht den Nutzer bei der Registrierung zum Studienwahl-Navigator darauf aufmerksam, dass sich bereits 100'000 Sudierende namentlich registriert haben und 200'000 die Umfrage anonym ausgefüllt haben, wie in Abbildung 76 gezeigt wird. Dies weist auf einen qualitativ hochstehenden Online-Service hin, der den Studierenden bei der Entscheidung zur richtigen Studienwahl weiterhelfen kann. Auf den Sozialen wirkt diese Angabe sehr überzeugend. Ebenso der Hinweis, dass der Nutzer die Wahlfreiheit zwischen namentlicher und anonymer Registerierung hat, ist für den Sozialen von Bedeutung, wie wir noch beim Faktor Reziprozität sehen werden.

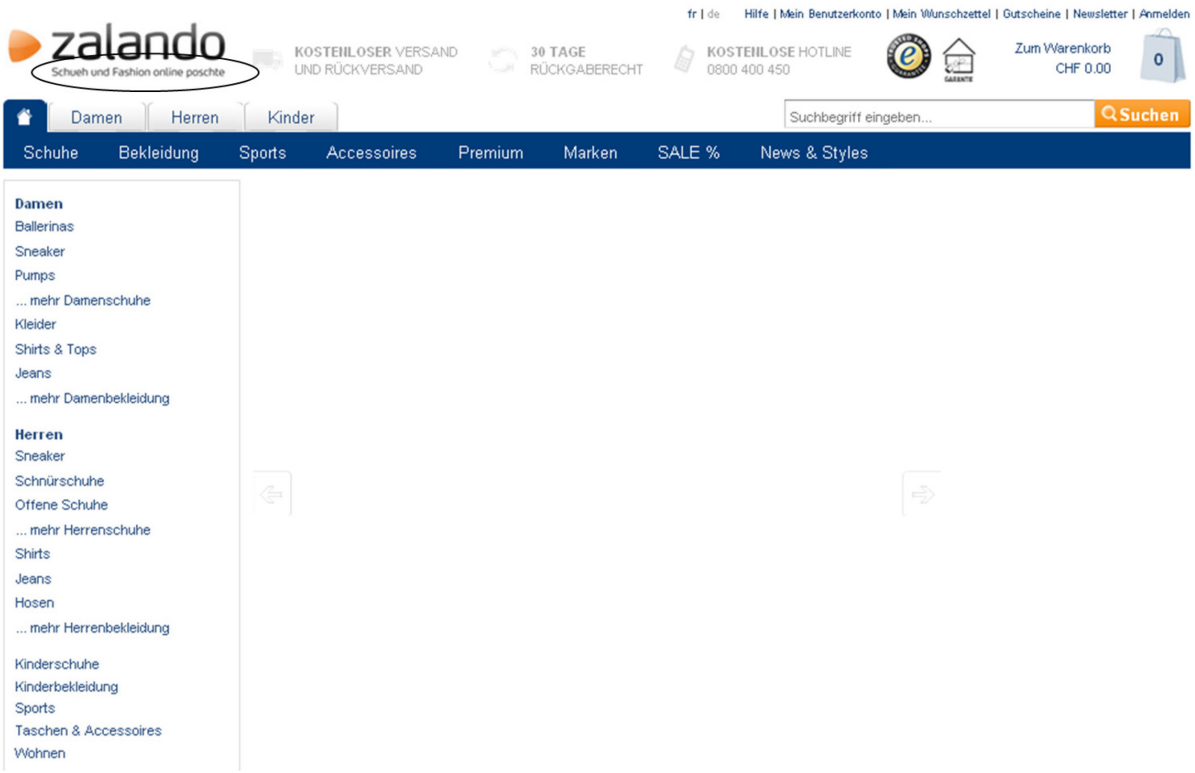


Abbildung 77: Schlichtes Design und schweizerdeutscher Slogan bei Zalando (Zalando, 2012)

Für den Sozialen ist es zentral, dass er sich auf der Seite des Anbieters wohlfühlt (V_103, Ø 1.89). Der Online-Versandhändler für Schuhe und Mode Zalando zum Beispiel passt seinen Slogan der jeweiligen Landessprache an. In der Deutschschweiz lautet der Slogan: „Schueh und Fashion online poschte“ (Abbildung 77). Dieser Hinweis auf die regionale Verwurzelung des Unternehmens fällt dem Sozialen sofort auf, wirkt auf ihn sympathisch und kann sein Wohlbefinden auf der Webseite positiv beeinflussen. Auffallend bei der Seite von Zalando ist ausserdem, dass kein einziges Produkt auf der Startseite abgebildet ist (Abbildung 77). Der Internetauftritt ist äusserst schlicht und übersichtlich gestaltet und lenkt den Blick des Sozialen auf die relevanten Links, welche dadurch überaus gut erkenntlich und mit genügend Hintergrundinformationen verknüpft sind (V_100, Ø 1.82; V_101, Ø 2.07). Ausserdem fühlt sich der Soziale bei überladenen Internetseiten tendenziell überfordert und kann Relevantes von Irrelevantem nicht sofort unterscheiden. Auch der Bestellablauf bei Zalando ist für den Sozialen logisch aufgebaut (V_102, Ø 1.87). Dass es Zalando nicht nötig hat, bereits auf der Frontseite mit Bestsellern und Schnäppchen zu werben, könnte für den Sozialen wiederum ein Hinweis darauf sein, dass der Anbieter bereits bekannt ist und einen genügend grossen Kundenstamm hat, was einen seriösen und professionellen Eindruck hinterlässt (V_98, Ø 1.95).

Um sich den Anbieter und die Marke einfacher zu merken, kann dem Sozialen eine Geschichte über das Unternehmen helfen. Soziale Medien leben vom Erzählen von Geschichten, sie sind eingängig und verbreiten sich innerhalb sozialer Netzwerke sehr schnell. Dies kann einer der Gründe sein, weshalb das soziale Netzwerk Facebook sich weltweit so rasant ausgebreitet hat. Hinter der Gründung des Unternehmens Facebook steht die Sehnsucht nach einem Partner, aber ebenso eine spannende Geschichte voller Intrigen, Diebstahl und Verrat. So spannend, dass sie sogar von Hollywood aufgenommen und verfilmt wurde[52]. Noch heute ist die Gründungsgeschichte von Facebook nicht voll aufgearbeitet und bietet viel Platz für Spekulation: "The success of a corporate story can be measured by the many ways in which different people (…) tell that story." (van Riel & Fombrun, 2007, S. 148). Über Geschichten lassen sich Informationen wie zum Beispiel Marken und deren Assoziationen am leichtesten in den Köpfen der Mitarbeiter und Kunden verankern. Es könnte sein, dass auch der Soziale eine Gründergeschichte schätzt, da für ihn das Unternehmen greifbarer wird und ihm dadurch seine soziale Komponente offenbart wird.

Da ihm seine Mitmenschen am Herzen liegen, könnte es sein, dass er sich auch aktiv für Nachhaltigkeit engagiert. Insbesondere beim Kauf von Produkten achtet er auf einen fairen Umgang mit Menschen und auf einen ökologischen Umgang mit Ressourcen. Falls sich der Anbieter in diesem Bereich engagiert, kann dies sehr gut über die Marke oder in Kooperation mit Marken transportiert werden. Insbesondere bekannte Marken wie Max Havelaar fallen dem Sozialen umgehend auf. Das Online-Blumenversandhaus Fleurop zum Beispiel bietet Produkte an, welche durch das Zertifikat „Fair Trade von Max Havelaar" ausgezeichnet wurden und kommuniziert dies prominent auf der Homepage.

Kundenservice: Nicht alle Items des Faktors Kundenservice sind für den Sozialen relevant, nicht alle weisen einen Mittelwert kleiner 2.5 auf (Abbildung 78 & Anhang 7.6.1). Für den Sozialen stehen reale Menschen ganz klar im Mittelpunkt und Anbieter von Online-Geschäftsmodellen sollten versuchen, den Sozialen über die Gefühlsebene anzusprechen.

[52] Der Film „The Social Network" des amerikanischen Regisseurs David Fincher kam im Jahr 2010 in die Kinos.

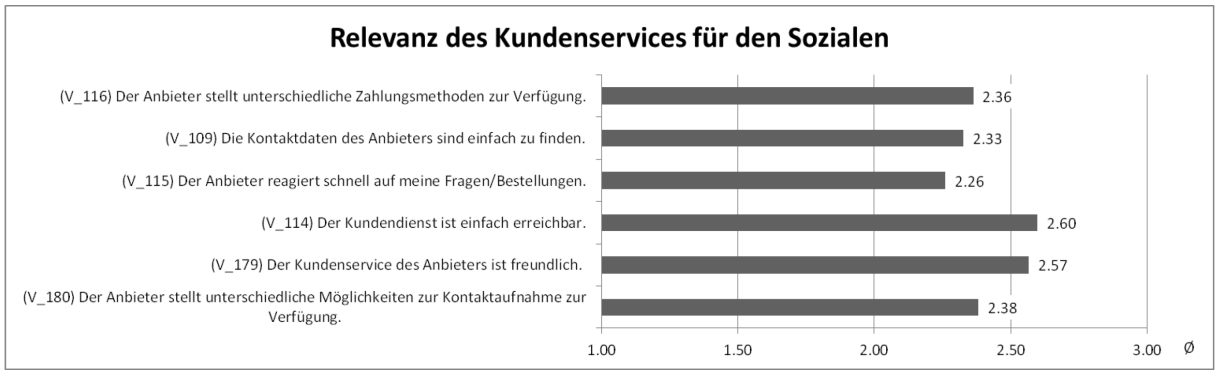


Abbildung 78: Mittelwerte der Items des Faktors Kundenservice des Sozialen (Interpretation: 1 „trifft zu“, 5 „trifft nicht zu“)

Der Soziale nutzt das Internet vergleichsweise selten und er ist im Umgang mit unterschiedlichen Geschäftsmodellen nicht geübt. Treten Unklarheiten auf, müssen diese sofort beseitigt werden, in einer Stunde ist er eventuell nicht mehr online und der Kunde hat sich zu einem anderen Anbieter geklickt. Der Soziale achtet deshalb beim Kundenservice insbesondere darauf, ob der Anbieter schnell auf Bestellungen oder Fragen reagiert (V_115, Ø 2.26). Eine prompte Bestätigung bei einer Bestellung ist für ihn ein Hinweis darauf, dass nicht in den luftleeren Raum bestellt wurde. Umgehend nach einer Bestellung sollte demnach beim Kunden eine Bestätigung eintreffen, was technisch einfach per SMS oder per E-Mail möglich ist. Dadurch hat der Kunde ohne Aufwand bereits eine erste Kontaktmöglichkeit bei eventuellen Rückfragen. Darüber hinaus kann der Kunde über den weiteren Verlauf der Bestellung informiert werden. Das Versandhaus Amazon zum Beispiel bestätigt jede Bestellung umgehend per E-Mail und informiert, wenn die Bestellung zum Versand aufgegeben wurde. Dadurch ist der Soziale immer über den Stand der Bestellung informiert, fühlt sich gut betreut und ernst genommen.

Bei der Interpretation der Vertrauenstypen (Kapitel 4.1.3.1) haben wir gesehen, dass es für den Sozialen zentral ist, dass reale Menschen hinter einem Angebot stehen, denen er sein Vertrauen schenken kann. Anbieter von Online-Geschäftsmodellen könnten ihr Kundenservice-Team auf der Seite mit Foto und Beschreibung kurz vorstellen. Gelingt es dem Anbieter, einen sympathischen Eindruck zu hinterlassen, wird der Soziale bei offenen Fragen mit grosser Wahrscheinlichkeit den Kundenservice mit einer positiven Einstellung kontaktieren, was auf den gesamten Beratungsablauf Einfluss haben wird.

Ausserdem könnten für den Sozialen Avatare eingesetzt werden, um den Umgang mit der Seite möglichst einfach zu erlernen. Ein schönes Beispiel für den Einsatz ei-

nes solchen grafischen Stellvertreters findet sich auf der Internetseite des deutschen Salzlandkreises. Der Salzlandkreis ist eine Gebietskörperschaft im Bundesland Sachsen-Anhalt und hat 2006 zu Standortmarketingzwecken das Online-Portal Salzlandkreis.net ins Leben gerufen. Die Seite etablierte sich schnell, erweiterte sich und wurde zunehmend unübersichtlich. Deshalb wurde Pia eingesetzt, ein Avatar für den virtuellen Support der Seitennutzer, abgebildet in Abbildung 79. Pia stellt dem Nutzer das Portal vor, findet Inhalte und erklärt den Aufbau und die Navigation auf der Seite. Auch das Möbelhaus IKEA setzt erfolgreich den Avatar Anna bei Kundenfragen ein (IKEA, 2012). Da sich der Soziale einen zeitnahen Kundenservice auch online wünscht, eignet sich der Einsatz von Avataren besonders für diesen Vertrauenstyp.

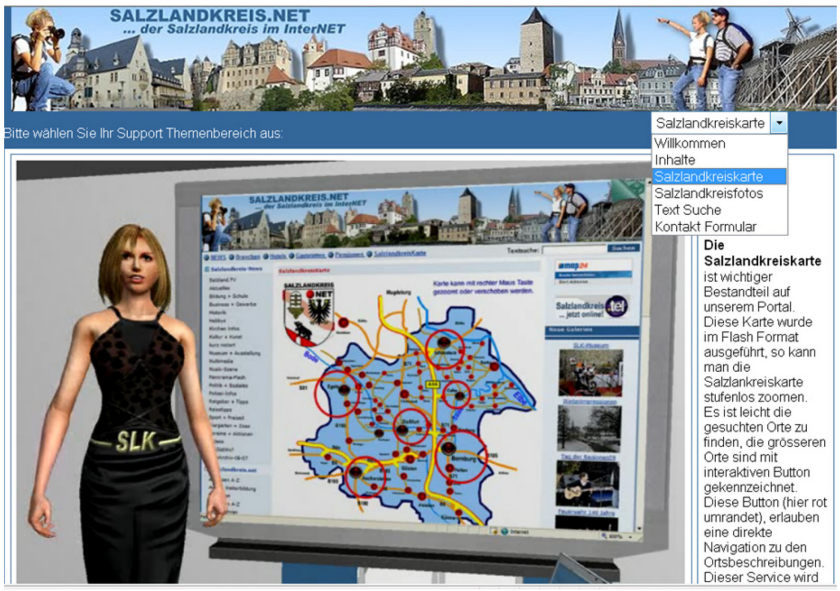


Abbildung 79: Avatar als Kundensupport beim Salzlandkreis (Salzlandkreis, 2012)

Wenn der Soziale den Kundenservice kontaktieren will, müssen dessen Kontaktinformationen einfach zu finden sein (V_109, Ø 2.33). Er erwartet einen „Kontakt"-Link, bei dem die unterschiedlichen Möglichkeiten der Kontaktaufnahme aufgelistet sind (V_180, Ø 2.38). Da der Soziale mehr Vertrauen in Menschen als in Maschinen hat, ist es wahrscheinlich, dass er sich am liebsten persönlich mit einem Servicemitarbeiter bespricht. Der Marketer Emanuel Rosen stellte fest: "The greatest advertising medium of them all is the human voice." (2009, o. S.). Dies trifft nicht nur auf Word-of-Mouth zu, sondern auch auf den Kundenservice. Der Soziale schätzt den direkten Kontakt zu Menschen, denn so kann er sichergehen, dass sein Anliegen richtig verstanden wird und dass alle seine Fragen beantwortet werden. Dies muss aber nicht immer von Angesicht zu Angesicht oder per Telefon sein, sondern kann ebenso über

einen Chat stattfinden, wie dies der Vermittler für Kurierlieferdienste EAT.ch anbietet (Abbildung 80).

Abbildung 80: Live Chat Support nach den Bürozeiten (Eat, 2012)

Um Spitzenzeiten beim Abendessen zwischen 17.30 und 21.30 Uhr abdecken zu können, hat der Online-Anbieter EAT.ch einen Live Chat Support eingerichtet. Denkbar ist auch ein Chat Support von Nutzer zu Nutzer, wenn der Anbieter bereits etabliert und die Fangemeinschaft gross genug ist (Customer to Customer Care). Eine Möglichkeit, Nutzer zur Partizipation zu animieren, ist das Einrichten einer Community oder eines Forums (Casalo et al., 2008). Darauf können sich Nutzer untereinander austauschen, sich über das Produkt oder die Plattform unterhalten und sich bei Fragen gegenseitig weiterhelfen. Dadurch kommt der Soziale an für ihn relevante und glaubwürdige Informationen aus erster Hand. Auch Mitarbeiter und Geschäftsleitung können im Namen der Firma an der Diskussion teilnehmen. Einzelne Auszüge aus den Chatprotokollen könnten als Empfehlungen in Echtzeit genutzt werden. Der Soziale kann dadurch Teil einer Community werden, mit den Mitgliedern diskutieren und mitbestimmen. Dieser Aspekt des Gemeinsamen ist für den Sozialen sehr wichtig, dadurch fühlt er sich vom Unternehmen verstanden. Das Detailhandelsunternehmen Migros zum Beispiel stellt seinen Kunden die Kommunikationsplattform Migipedia zur Verfügung. Auf diesem Forum können sich Konsumenten untereinander über Themen rund um die Migros austauschen, Produkte bewerten oder Vorschläge einbringen. Die Betreiberin streamt aktuelle Kommentare der Nutzer direkt auf die Frontseite und hebt seine aktivsten Benutzer hervor, wie in Abbildung 81 zu sehen ist. Eine Voraussetzung dafür ist, dass die einzelnen Beiträge breit gestreut sind und nach dem Zufallsprinzip ausgewählt werden. Werden nur handverlesene, positive Beiträge übernommen, leidet die Glaubwürdigkeit und somit der Effekt der Empfehlungen.

Abbildung 81: Animation zur Nutzerpartizipation bei Migipedia (Migipedia, 2012)

Da der Soziale im Netz etwas unsicher ist, kann eine obligatorische Aktivierung des Nutzerkontos bei einer Online-Registrierung sinnvoll sein. Erstens zeigt es ihm, dass die Angaben (oder zumindest die E-Mail-Adressen der anderen Nutzer) kontrolliert werden, und zweitens gibt es ihm einen Hinweis darauf, ob das Unternehmen gut strukturiert ist und Interesse an der Identität seiner Nutzer hat.

Es überrascht besonders, dass dem Sozialen ein freundlicher Kundenservice nicht überdurchschnittlich wichtig ist (V_179, Ø 2.57). Eigentlich wurde erwartet, dass Freundlichkeit für den Sozialen ein zentrales Anliegen ist, bei dem der Anbieter sich profilieren könnte. Dies könnte daran liegen, dass Freundlichkeit gegenüber Kunden für den Idealisten und Menschenfreund eine so selbstverständliche Eigenschaft ist, dass er diese nicht explizit betont.

Reziprozität: Alle Items des Faktors Reziprozität sind für den Sozialen relevant. Wie in Abbildung 82 (sowie im Anhang 7.6.1) zu sehen ist, weisen alle Items einen Mittelwert kleiner 2.5 auf, einige jedoch nur sehr knapp. Der Soziale schaut zwar, dass er nicht übervorteilt wird, und achtet auf ein angemessenes Austauschverhältnis, im Vordergrund steht für ihn jedoch die Erfahrung, damit er mit seinem sozialen Umfeld über das Erlebte diskutieren und mitreden kann. Weil die soziale Komponente des Mitdabeiseins zentraler ist als das Reziprozitätsverhältnis, erscheint dieser Faktor eher am Schluss seiner Prioritätenliste.

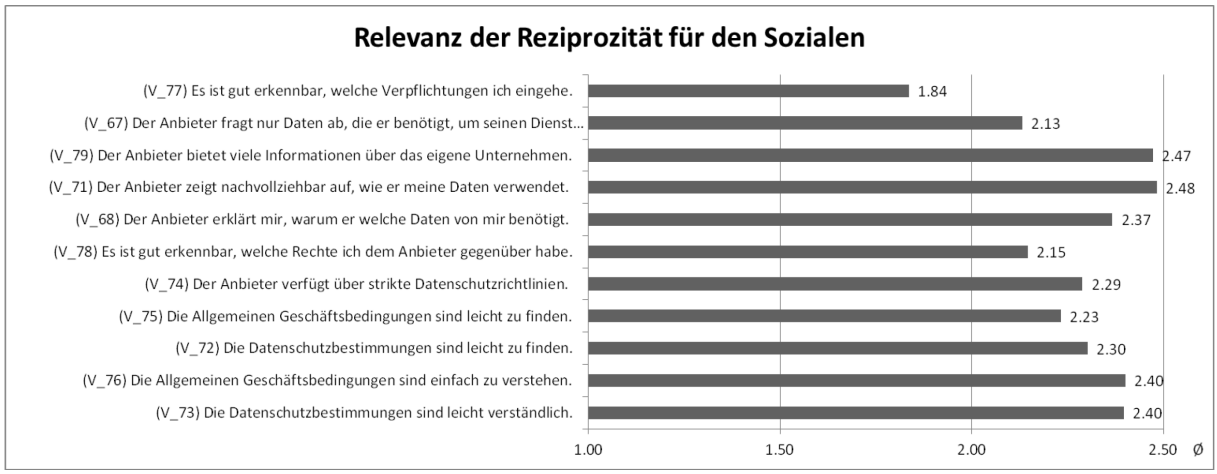


Abbildung 82: Mittelwerte der Items des Faktors Reziprozität des Sozialen (Interpretation: 1 „trifft zu“, 5 „trifft nicht zu“)

Besonders wichtig ist für den Sozialen, dass er weiss, auf was er sich bei einem Vertragsabschluss einlässt. Es muss demnach gut erkennbar sein, welche Verpflichtungen er beim jeweiligen Anbieter mit der Transaktion eingeht (V_77, Ø 1.84). Nicht dass zum Beispiel bei einer internationalen Bestellung unerwarteterweise noch Zollkosten oder Mehrwertsteuer aufaddiert werden. Um sich für ein Angebot enscheiden zu können, möchte der Soziale den Totalbetrag der zu tragenden Kosten vor dem Vertragsabschluss verbindlich vorliegen haben. Die Plattform für den Kauf und Verkauf von handgemachten Produkten DaWanda zum Beispiel weist explizit darauf hin, dass der Vertrag mit dem jeweiligen Käufer abgeschlossen wird und nicht mit der Plattform DaWanda selbst: „Bestellung bei Verkäufer XY“ sowie „Kauf erfolgt unter Einbeziehung der AGB des Verkäufers.“, wie in Abbildung 83 zu sehen ist. Die AGBs können auf dieser Seite mit einem Klick überprüft werden. Darin ist klar ersichtlich, welche Garantien oder Rückgaberechte dem Anbieter gegenüber bestehen (V_78, Ø 2.15). Der Soziale weiss nun, wer sein Vertragspartner ist. Er kann die Waren innerhalb von 30 Tagen ohne Angabe von Gründen retournieren und erhält den vollen Verkaufspreis zurückerstattet.

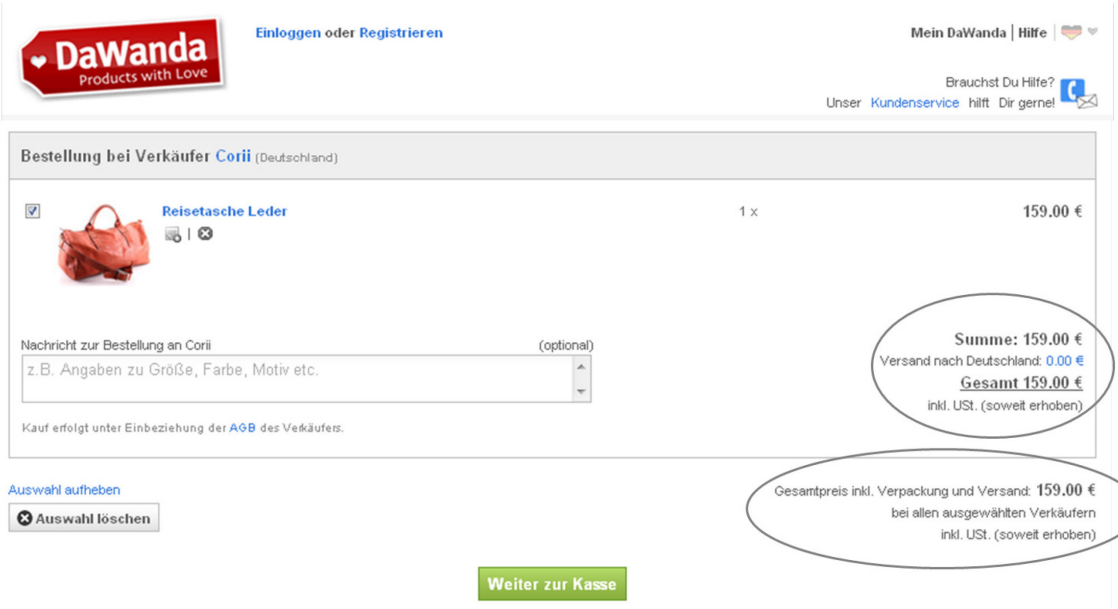


Abbildung 83: Verpflichtungen bei DaWanda (DaWanda, 2012)

Ausserdem ist bei DaWanda gut ersichtlich, was im Gesamtpreis enthalten ist: Mehrwertsteuer, Verpackung und Versand sind im Endpreis inbegriffen. Zusätzliche Kostenpunkte und unangenehme Überraschungen sind bei DaWanda eher keine zu erwarten.

Die Austauschbeziehung muss fair für beide Parteien sein. Ansonsten besteht für den Sozialen schnell der Verdacht, dass es sich um ein unseriöses Angebot handelt; er weiss, dass es nichts umsonst gibt. Wenn seiner Meinung nach das Reziprozitätsverhältnis ungleich verteilt ist, sucht der Soziale nach Zusatzinformationen über den Anbieter. Dies kann auf der Homepage des Anbieters, aber auch über Suchmaschinen auf Drittseiten sein. Dann liest er die Datenschutzbestimmungen und die AGBs, um eine Erklärung für die seiner Meingung nach ungleiche Austauschbeziehung zu finden. Es könnte sein, dass der Soziale zum Beispiel auch deshalb vergleichsweise selten auf sozialen Netzwerken anzutreffen ist (wie in Anhang 7.5.7 ersichtlich, nutzt er zu 26.9 % „nie“ soziale Netzwerke). Die Datenpreisgabe, die Unsicherheiten durch die stetigen Veränderungen der Datenschutzrichtlinien und die fehlenden gesetzlichen Bestimmungen halten ihn nach wie vor vom regelmässigen Gebrauch sozialer Netzwerke ab.

Das sich lohnende Reziprozitätsverhältnis kann auch von anderen Internetnutzern bestätigt werden. Besonders für den Sozialen spielen Erfahrungen von Nutzern eine wichtige Rolle bei der Beurteilung der Vertrauenswürdigkeit eines Anbieters. Die

Online-Partnervermittlung Parship zum Beispiel setzt auf die Erfolgsgeschichten ihrer bisherigen Nutzer und publiziert „Echte Geschichten der wahren Liebe“ prominent auf ihrer Homepage (Abbildung 84). Dass die Erfolgsgeschichten eine Sogwirkung für unentschlossene Kunden haben, wurde von vielen Online-Anbietern erkannt.

Abbildung 84: Erfolgsgeschichten bei Parship (Parship, 2012)

In diesem Kapitel haben wir die relevanten Vertrauensfaktoren pro Vertrauenstyp im Detail diskutiert. Die Forschungsfrage „Sind während einer Transaktion im Internet für die unterschiedlichen Vertrauenstypen dieselben Vertrauensfaktoren relevant?“ konnte klar beantwortet werden, die Vertrauensfaktoren unterscheiden sich signifikant nach Typ. Konkrete Handlungsempfehlungen für Anbieter von Online-Geschäftsmodellen werden im Kapitel 5.2.2 vorgestellt. Im folgenden Kapitel werden nun die Vertrauensabsichten im Detail betrachtet.

4.3 Jeder reagiert anders: Vertrauensabsichten pro Vertrauenstyp

Dieses Kapitel diskutiert die dritte Forschungsfrage: „Unterscheiden sich die Vertrauenstypen in Bezug auf ihre Vertrauensabsichten?“ Im Methodik-Kapitel 3.2.3 wurde anhand des Kruskal-Wallis-Tests (Tabelle 17) festgestellt, dass sich die drei Vertrauenstypen nicht anhand des Faktors Vertrauensabsicht unterscheiden lassen.

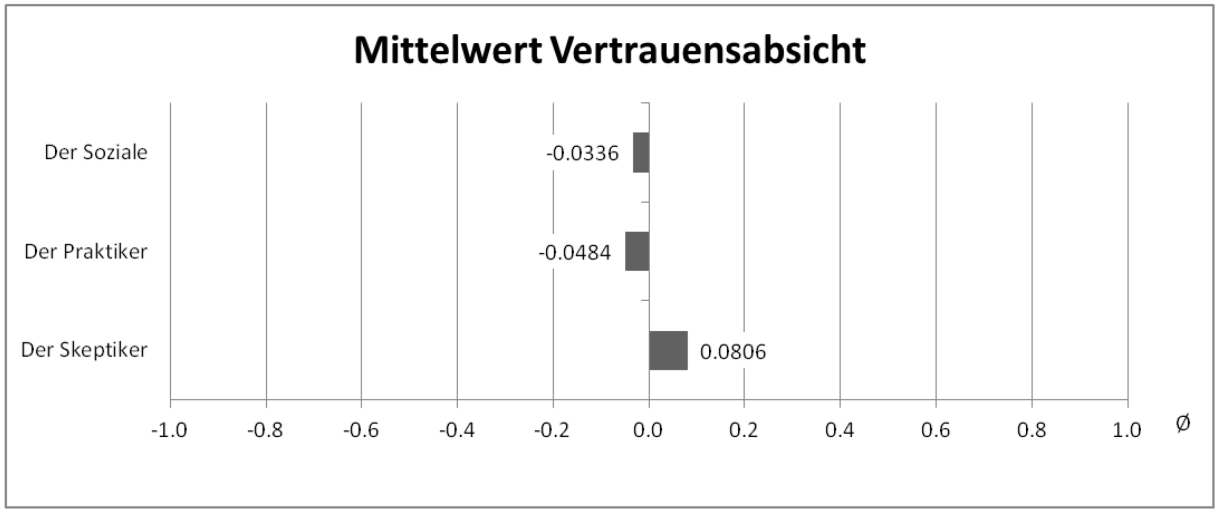


Abbildung 85: Mittelwertvergleich der Vertrauenstypen anhand des Faktors Vertrauensabsicht (Interpretation: negative Werte tendieren zu „trifft zu“, positive Werte zu „trifft nicht zu“)

Abbildung 85 zeigt die Mittelwerte der drei Vertrauenstypen. Bei der Interpretation der Mittelwerte des Faktors Vertrauensabsicht ist zu erwähnen, dass negative Abweichungen eine Tendenz in Richtung „trifft zu“ und positive Werte eine Tendenz in Richtung „trifft nicht zu“ im Vergleich zum gesamten Sample andeuten. In der Grafik wird ersichtlich, dass sich die Mittelwerte sehr stark um den Nullpunkt herum bewegen, und dieser Mittelwertvergleich bestätigt die aus dem Kruskal-Wallis-Test hervorgehende geringe Signifikanz. Alle drei Vertrauenstypen haben positive Vertrauensabsichten, der Unterschied zwischen den Typen jedoch ist nicht signifikant.

Wenn sich der Nutzer einmal entschlossen hat, einem Anbieter gegenüber persönliche Daten preiszugeben, und wenn die Transaktion fehlerfrei und erfolgreich verlaufen ist, wird der Nutzer in Zukunft mit einer hohen Wahrscheinlichkeit die Seite wieder besuchen. Nach Durchlaufen des Entscheidungsfindungsprozesses sinkt das persönlich empfundene Risiko gegenüber diesem Anbieter und eine erneute Trans-

aktion ist viel eher wahrscheinlich. Dies könnte ein Grund dafür sein, weshalb der Faktor Vertrauensabsicht bei den drei Vertrauenstypen stark ausgeprägt ist und deren Mittelwerte relativ nahe beieinander liegen. Für Anbieter von Online-Geschäftsmodellen heisst das, dass insbesondere in die Vertrauensbildung vor und während des Entscheidungsfindungsprozesses investieren werden sollte, da die zukünftige Vertrauensabsicht bei erfolgreichen Transaktionen tendenziell positiv ist.

Es scheint, dass Menschen dazu neigen, einmal getroffene Entscheidungen im Nachhinein nicht negativ zu bewerten. Der Grund dafür könnte darin liegen, dass sich Internetnutzer sehr bewusst bei einem bestimmten Geschäftsmodell registrieren und sich für jenen Anbieter entscheiden, der ihrem Bedürfnis am ehesten entspricht. Jeder Nutzer weist ein bestimmtes Vertrauensprofil auf und bewegt sich entsprechend in dem für ihn akzeptablen Internetumfeld und wählt darin einen entsprechenden Anbieter. Das heisst, dass eine Person, welche zum Beispiel sozialen Netzwerken im Allgemeinen misstraut, sich bei dieser Umfrage eher weniger bei einem sozialen Netzwerk neu registriert hat. Es scheint, dass Personen sich viel eher in einem Internetumfeld bewegen, welches ihrem Vertrauensprofil entspricht.

Es könnte sein, dass sich die drei Vertrauenstypen aufgrund der Vertrauensabsicht signifikant unterscheiden lassen würden, wenn die Probanden einem bestimmten Online-Geschäftsmodell zugeteilt worden wären. Bei dieser Umfrage durften die Probanden denjenigen Anbieter wählen, bei dem sie sich zuletzt registriert haben. Man kann davon ausgehen, dass der Grossteil der Teilnehmer den Prozess der Registrierung auch abgeschlossen hat. Die Umfrage beinhaltet demnach vor allem Geschäftsmodell-Anbieter, bei welchen sich die Nutzer bis zur Vollendung der Transaktion sicher gefühlt haben, ansonsten hätten sie die Registrierung abgebrochen. Dies könnte ein Hinweis für die durchgängig hohe Bewertung des Faktors Vertrauensabsicht sein. Ein möglicher weiterer Grund für die fehlende Signifikanz könnte auch darin liegen, dass dieser Faktor nur aus drei Items besteht und sich eine Verzerrung der Antworten im „Trifft zu“ Bereich abzeichnet. Im Folgenden werden die drei Items und deren Bedeutung für Anbieter von Online-Geschäftsmodellen kurz diskutiert.

Das Item V_61 „Ich werde die Seite des gewählten Anbieters wahrscheinlich wieder besuchen.“ beinhaltet keine Zeitangabe. Gefragt wurde demnach, ob es möglich ist, dass die befragte Person irgendwann einmal wieder auf dieser Seite anzutreffen sein wird. Insbesondere bei teuren Einzelanschaffungen, zum Beispiel bei Luxusgütern oder einer Investition, kann nicht im Voraus gesagt werden, wann wieder eine

Transaktion abgeschlossen wird. Ebenso bei Dating-Plattformen: Hat der Befragte seine Liebe gefunden, wird er mit grosser Wahrscheinlichkeit in den nächsten Monaten nicht auf der Plattform anzutreffen sein, aber eventuell in einem halben Jahr bereits wieder. Bei Online-Angeboten mit hohem kognitivem Aufwand zur Registrierung oder beim Kauf von teureren Produkten oder Dienstleistungen sind Zeitangaben schwierig abzuschätzen und dies könnte der Grund für die Verzerrung dieses Items sein.

Das Item V_62 „Ich werde die Dienste des gewählten Anbieters in den nächsten 3 Monaten erneut in Anspruch nehmen." deckt eine im Internet absehbare Zeitspanne ab. Drei Monate sind auch in dieser schnelllebigen Umgebung berechenbar. Nimmt ein Nutzer einen Dienst in Anspruch, ist dies wesentlich konkreter als die Seite nur „wieder zu besuchen". Soziale Netzwerke, Blog- und Microbloggingdienste würden nicht funktionieren, wenn ihre Nutzer nur halbjährlich ihr Profil updaten und Beiträge lesen und schreiben würden. Auch Lebensmittellieferdienste wie coop@home.ch oder LeShop.ch sind auf Wiederkäufer angewiesen. Repetitive Einkäufe kommen besonders bei Produkten oder Dienstleistungen ohne hohen kognitiven Aufwand vor, wie dies bei Konsumgütern der Fall ist. Dieses Item ist insbesondere für Anbieter interessant, welche auf regelmässige Interaktionen mit dem Nutzer setzen. Dies können zum Beispiel Community-Plattformen sein oder aber Anbieter von Verbrauchsgütern. Es ist demnach sehr wahrscheinlich, dass Nutzer von sozialen Netzwerken, Blogs oder Online-Shops mit Konsumgütern die Seite in den nächsten drei Monaten wieder in Anspruch nehmen werden und sich deshalb auch hier eine Verzerrung der Antworten im Bereich „trifft zu" abzeichnet.

Das Item V_63 „Ich würde die Seite des gewählten Anbieters anderen Personen weiterempfehlen." unterscheidet nicht, ob die Weiterempfehlung im realen Leben oder im Internet stattfindet. In der Offline-Welt, zum Beispiel im Freundes- oder Bekanntenkreis, empfiehlt man einen aussergewöhnlich guten oder warnt vor einem schlechten Dienstleister (Kimmel, 2010). Die Empfehlung erreicht nicht viele Personen, dafür hat sie aber eine grosse Gewichtung, da sie meistens von Vertrauenspersonen stammt. In der virtuellen Welt können schneller viele Menschen erreicht werden. Durch das „Liken" eines Anbieters oder einer Marke in einem sozialen Netzwerk wie Facebook sehen diese Empfehlung Hunderte von Freunden, und diese können die Empfehlung wiederum weitertragen. Die Art und auch der Aufwand einer Weiterempfehlung können sehr unterschiedlich sein. Es kommt darauf an, ob der Nutzer unter Weiterempfehlung eine Empfehlung im realen Leben, eine ausführ-

liche Kundenrezension oder das Klicken des Like-Buttons versteht. Auf Bewertungsplattformen wie zum Beispiel Yelp oder Trip Advisor spielt weniger die Meinung einer Einzelperson eine Rolle, sondern vielmehr die Durchschnittsbewertung der Masse. Auf Blogs können Erfahrungsberichte ausformuliert und mit Bildern, Videos oder Links bereichert werden. Deshalb ist es für Online-Anbieter besonders relevant, dass extrovertierte, internetaffine Meinungsführer dieses Item positiv bewerten. Für Anbieter ist es besonders interessant, wenn Vertrauenstypen mit einer grossen, gut vernetzten Community ihr Angebot weiterempfehlen, da hier die Netzwerkeffekte[53] voll zum Tragen kommen können. Da es sich bei dieser Umfrage zum grössten Teil um erfolgreich abgeschlossene Registrierungen handelt, ist die Chance höher, dass Nutzer den Anbieter und dessen Angebot auch weiterempfehlen. Dies könnte ein Grund für die hohe „Trifft zu"-Quote sein.

Diese Studie konnte aufzeigen, dass sich die drei Vertrauenstypen aufgrund der fehlenden Signifikanz durch den Faktor Vertrauensabsicht nicht unterscheiden lassen. Mithilfe der bisherigen Typen-Charakteristiken können jedoch Tendenzen in Bezug auf die Vertrauensabsicht ausgemacht werden, die in den folgenden drei Kapiteln diskutiert werden.

4.3.1 Vertrauensabsichten des Skeptikers (Vertrauenstyp 1)

Das Antwortverhalten des Skeptikers bei Fragen zu den Vertrauensabsichten zeigt, dass er bei allen drei Fragen am wenigsten „trifft zu" oder „trifft eher zu" angekreuzt hat (siehe Anhang 7.7.1: V_61 zu 80.2 %; V_62 zu 74.7 %; V_63 zu 54.6.6 %). Betrachten wir die bisherigen Analysen des Skeptikers, ist dieses Antwortverhalten völlig schlüssig. Der Skeptiker lässt sich im Vergleich am wenigsten darauf ein, sich in ferner Zukunft auf einen im Voraus definierten Anbieter zu verlassen. Er ist gut gebildet und weiss, dass sich die Marktverhältnisse schnell ändern können und neue Anbieter in den Markt drängen werden. Wie wir im Kapitel 4.1.1.2 gesehen haben, kann sich der Skeptiker für ihn relevante Information im Internet problemlos beschaffen (85.5 % „trifft zu" oder „trifft eher zu"). Möchte er einen Service in An-

[53] Unter einem Netzwerkeffekt spricht man, wenn ein positiver externer Effekt entstehet: Mit einer steigenden Zahl an Teilnehmern steigt der Nutzen für sämtliche Teilnehmer exponentiell an (Haes, 2003).

spruch nehmen oder ein Produkt kaufen, analysiert er den Markt zu diesem Zeitpunkt und entscheidet sich für den seiner Meinung nach besten Anbieter. Relativ unabhängig von seinen eigenen bisherigen Erfahrungen beurteilt er die Situation jeweils aufs Neue. In Abbildung 45 ist zu sehen, dass der Skeptiker im Vergleich wenig Vertrauen in den Anbieter hat. Er hat Angst, dass er vom Anbieter übervorteilt wird, falls er nicht aufpasst. Auch Marken und der Kundenservice spielen für ihn eine untergeordnete Rolle bei der Entscheidungsfindung.

Der Skeptiker scheint keine starke emotionale Bindung zum Anbieter zu haben und bei solch einem Vertrauenstyp ergibt es im Vergleich am wenigsten Sinn, in Beziehungsmarketing und Customer-Relationship-Programme zu investieren.

4.3.2 Vertrauensabsichten des Praktikers (Vertrauenstyp 2)

Bei der prozentualen Betrachtung der Antworten des Praktikers sind die positiven Vertrauensabsichten ganz klar ersichtlich: Ob er die Seite wieder besucht, hat er zu 96.2 % mit „trifft zu“ oder „trifft eher zu“ beantwortet. Auch beeindruckend ist, dass er die Seite zu 88.4 % in den nächsten drei Monaten erneut in Anpruch nehmen wird und die Seite zu 88.8 % weiterempfielt („trifft zu“ oder „trifft eher zu“) (Anhang 7.7.1). Der Praktiker wird demnach mit hoher Wahrscheinlichkeit die Seite des Anbieters erneut ansteuern. Diese hohe Bereitschaft, den Anbieter wieder in Anspruch zu nehmen, ist besonders für Anbieter von Verbrauchsgütern und bei Seiten mit hoher Nutzerinteraktion wichtig. Der Aufwand des Anbieters, ihn zu einer weiteren Transaktion zu überzeugen, ist viel geringer als bei der Erstregistrierung. Betrachten wir nochmals die konkret gewählten Online-Anbieter des Praktikers in Abbildung 96, fallen besonders eBay und Amazon auf, beide Anbieter von Verbrauchsgütern. In Abbildung 49 ist ersichtlich, dass das Vertrauen in den Anbieter wie auch in die Institution Internet beim Praktiker sehr hoch sind. Ist der Praktiker mit einem Anbieter zufrieden, zieht er ihn mit sehr hoher Wahrscheinlichkeit wieder in Betracht.

Der Praktiker verbringt gerne viel Zeit im Netz und es macht ihm Spass, neue Seiten auszuprobieren. Er kann sich leicht im Netz orientieren und weiss, welche neuen Anbieter in der Zwischenzeit auf dem Markt sind. Stimmt das Reziprozitätsverhältnis für ihn noch immer, wird er sich für den ihm bekannten Anbieter entscheiden. Ändert sich aber zum Beispiel der Preis markant, wechselt der Praktiker höchst wahrscheinlich den Anbieter.

Wie wir gesehen haben, ist die Bereitschaft des Praktikers gross, den Anbieter anderen Personen weiterzuempfehlen. Dass ihm die Möglichkeit gegeben wird, den Anbieter zu bewerten, gibt ihm ein gutes Gefühl. Beim Praktiker lohnt es sich besonders, in den Aufbau einer Beziehung zu investieren. Nicht nur aufgrund der erneuten Transaktion, sondern ebenso aufgrund seiner hohen Bereitschaft, einen guten Service oder Anbieter in seiner Community weiterzuempfehlen. Er schätzt seine Internetkompetenzen als sehr hoch ein und ist viel auf verschiedenen Plattformen anzutreffen. Der Praktiker hat das Potenzial, ein Meinungsführer im Netz zu sein, zum Beispiel über seinen eigenen Blog oder über seine grosse und diverse Community. Wenn er den Anbieter auf diesen Plattformen weiterempfiehlt, ist die Chance am höchsten, dass diese Weiterempfehlung auch beachtet wird.

Stimmen für den Praktiker die Leistungen eines Anbieters, ist er ein überaus loyaler und kanaltreuer Internetnutzer.

4.3.3 Vertrauensabsichten des Sozialen (Vertrauenstyp 3)

Bis jetzt konnte festgestellt werden, dass der Soziale im Vergleich eher kein Vertrauen in die Institution Internet, dafür aber in den Anbieter selbst hat. Er braucht relativ lange, bis er Transaktionen aus dem realen Leben ins Internet trägt, wie etwa seine niedrige Online-Banking- und Online-Shopping-Rate bestätigt (Kapitel 4.1.3.2). Hat sich der Soziale jedoch für einen Anbieter entschieden und ist er mit dessen Leistung zufrieden, bleibt er mit grosser Wahrscheinlichkeit ein treuer Stammkunde, wie die Antworten bei den drei Fragen zur Vertrauensabsicht bestätigen (siehe Anhang 7.7.1: V_61 zu 93.5 %; V_62 zu 83.5 %; V_63 zu 80.6 % „trifft zu“ oder „trifft eher zu“). Der Aufwand und das Risiko, bei jeder Transaktion alle Anbieter erneut in Betracht zu ziehen, sind dem Sozialen zu gross.

Es scheint, dass sich der Soziale stark an seinem sozialen Umfeld orientiert, auch bei seinen Internetaktivitäten. Es könnte demnach sein, dass wenn seine Community über einen bestimmten Anbieter spricht, der Soziale trotz positiver Erfahrungen den neuen Anbieter ausprobiert und dann eventuell wechselt. Mit dabei zu sein und mitreden zu können, ist ihm ein zentrales Anliegen.

Für Online-Anbieter ist es sehr aufwändig, den Sozialen als Neukunden zu gewinnen. Bei ihm muss intensive Überzeugungsarbeit geleistet werden. Hat er sich jedoch für einen Anbieter entschieden und ist er mit der Transaktion zufrieden, wird

er mit grosser Wahrscheinlichkeit ein treuer Abnehmer werden, obwohl er die Seite nicht sehr häufig besucht. Anbieter, welche auf repetitive Transaktionen setzen, können vom Sozialen profitieren. Er hat seine Lieblingsshops und Lieblingsseiten und bleibt diesen lange treu. Ist der Soziale mit einem Anbieter zufrieden, empfiehlt er diesen auch gerne seinen Freunden im realen Leben weiter und schreibt Online-Bewertungen. Dies ist insbesondere für Online-Anbieter interessant, welche auf dem Prinzip der gegenseitigen Kundenbewertungen basieren, wie zum Beispiel das Auktionshaus Ricardo[54].

Die dritte Forschungsfrage „Unterscheiden sich die Vertrauenstypen in Bezug auf ihre Vertrauensabsichten?“ muss verneint werden. Alle drei Typen haben positive Vertrauensabsichten, welche sich nicht signifikant voneinander unterscheiden lassen.

Im nächsten Kapitel werden die in diesem Kapitel diskutierten Ergebnisse zusammengefasst.

[54] Das Auktionshaus Ricardo stellt die Plattform zur Verfügung und die Nutzer der Seite kaufen voneinander und verkaufen aneinander. Ricardo selbst führt bei der Registrierung eine Identitätsprüfung auf dem Postweg durch, die Geschäfte werden aber unter den Ricardo-Nutzern ausgemacht. Betrug kann zwar an den Betreiber gemeldet werden, viel effektiver jedoch ist die Möglichkeit der gegenseitigen – und im Betrugsfall negativen – Bewertung.

4.4 Zusammenfassung

Die erste zu beantwortende Forschungsfrage „Existieren bei Internetnutzern unterschiedliche Vertrauenstypen?“ kann klar bejaht werden. Diese Studie unterscheidet drei Vertrauenstypen, wie in Abbildung 86 zusammengefasst.

Abbildung 86: Drei Vertrauenstypen auf einen Blick (eigene Darstellung)

(1) Der **Skeptiker** hat im Vergleich geringes Vertrauen in den Anbieter, eine tiefe allgemeine Vertrauensneigung und hat wenig Vertrauen in die Institution Internet. Er ist eher jünger und gehört somit zu den Digital Natives. Für ihn ist das Internet eine Selbstverständlichkeit und er fühlt sich wohl in der virtuellen Welt. Er ist sehr gut gebildet oder noch immer in Ausbildung. Er ist überaus oft auf sozialen Netzwerken anzutreffen und sucht auch häufig online nach Informationen. Es könnte sein, dass er seine sozialen Kontakte lieber schriftlich pflegt, um nicht von Mimik und Gestik verwirrt oder überfordert zu werden.

(2) Der **Praktiker** hat vergleichsweise grosses Vertrauen in den Anbieter und in das Internet, dafür hat er eine tiefe allgemeine Vertrauensneigung. Er ist eher älter und gehört zu den Digital Immigrants. Er hat einen Real- oder Berufsschulabschluss, ist fortschrittbegeistert, hat Freude am Vergleichen und ist eher preisbewusst. Er nutzt auffallend häufig Online-Games und hat sich zuletzt beim Online-Shopping oder beim Online-Banking neu registriert. Er nutzt das Internet zur Selbstverwirklichung und als Fenster zur Welt.

(3) Der **Soziale** vertraut anderen Menschen und seinem gewählten Anbieter, nicht aber der Institution Internet. Er fällt durch seine häufige Tendenz zur goldenen Mitte

auf und ist eher ein passiver Internetnutzer; dafür sind für ihn reale Menschen in seinem sozialen Umfeld wichtig.

Die zweite Forschungsfrage dieser Studie lautet: „Sind während einer Transaktion im Internet für die unterschiedlichen Vertrauenstypen dieselben Vertrauensfaktoren relevant?“ Die drei identifizierten Vertrauenstypen achten während einer Transaktion im Internet auf verschiedene Vertrauensfaktoren:

Für den **Skeptiker** sind keine der untersuchten vier Vertrauensfaktoren besonders relevant, wie in Abbildung 87 zu sehen ist. Werden die jeweiligen Items betrachtet, fällt auf, dass dem Skeptiker wichtig ist, dass er seine Verpflichtungen bei einem Transaktionsabschluss im Detail kennt. Ein weiteres Indiz zur Einschätzung der Vertrauenswürdigkeit ist für ihn das Alter sowie die Bekanntheit des jeweiligen Anbieters. Obwohl der Skeptiker eine im Vergleich eher sorglose Datenhandhabung aufweist, ist ihm wichtig, dass die Angabe von Daten über das notwendige Minimum hinaus freiwillig ist. Der Skeptiker ist nicht leichtgläubig, ihm muss der Online-Anbieter immer alles beweisen und mit Links versehen. Mit dem Kundenservice nimmt er am liebsten schriftlich Kontakt auf, weil er sich wohler fühlt, wenn er eine schriftliche Beweisgrundlage hat, und auch, um später immer wieder darauf zurückgreifen zu können.

Das Internet ist für den **Praktiker** mit einem Werkzeug zu vergleichen, welches er vor Gebrauch betrachten und prüfen möchte. Somit achtet er auch während einer Online-Transaktion auf alle vier Vertrauensfaktoren. Kosten-Nutzen-Überlegungen sind für ihn zentral und deshalb legt er Wert er auf ein ausgeglichenes Reziprozitätsverhältnis. Um die Vertrauenswürdigkeit eines Anbieters abzuschätzen, achtet er auf dessen Marke und das Design der Seite und erwartet zudem einen professionellen und freundlichen Kundenservice. Weiter ist es ihm ein wichtiges Anliegen, dass die Kontrolle über die persönlichen Daten bei ihm als Nutzer liegt.

Der **Soziale** achtet während einer Transaktion besonders auf die Marke und das Design eines Anbieters. Er bevorzugt bekannte, grosse und führende Anbieter mit einem grossen Kundenstamm. Er muss sich auf der Seite wohlfühlen, dazu gehört auch, dass das Design seriös wirkt. Die Kontaktdaten des Anbieters müssen leicht aufzufinden sein und er schätzt es, wenn ihm unterschiedliche Kontaktmöglichkeiten zur Auswahl stehen. Ausserdem achtet er auf ein faires Austauschverhältnis, er will ganz genau wissen, auf was er sich bei einem Angebot oder bei einer Registrierung einlässt.

Die relevanten Vertrauensfaktoren für den Skeptiker, den Praktiker sowie den Sozialen sind in Abbildung 87 nochmals zusammengefasst.

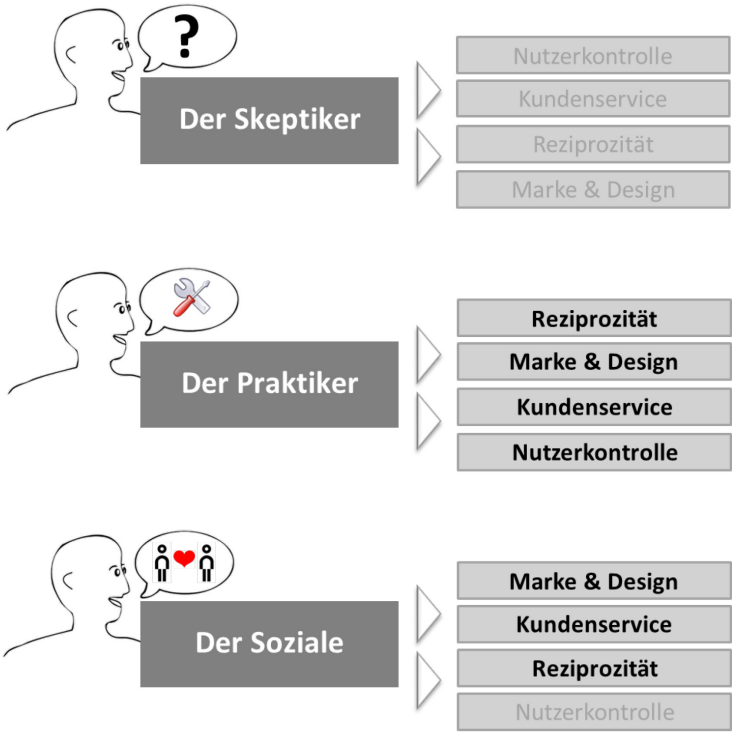


Abbildung 87: Zusammenfassung der Ergebnisse (eigene Darstellung)

Die dritte Forschungsfrage „Unterscheiden sich die Vertrauenstypen in Bezug auf ihre Vertrauensabsichten?“ muss verneint werden, die drei Vertrauenstypen lassen sich nicht anhand des Faktors Vertrauensabsicht unterscheiden. Alle drei Vertrauenstypen kommen mit grosser Wahrscheinlichkeit auf die Seite des Anbieters zurück und erwägen, die Dienste erneut in Anspruch zu nehmen. Haben sie positive Erfahrungen mit einem Anbieter gemacht, werden alle drei Vertrauenstypen die Seite wieder besuchen.

Im folgenden Kapitel wird auf die Schlussfolgerungen für das Vertrauensmanagement, die Forschungslimitationen und den Ausblick näher eingegangen.

5 Schlussfolgerung und Ausblick

Dieses abschliessende Kapitel steigt im Kapitel 5.1 ein mit den Schlussfolgerungen für die Vertrauensforschung, fasst in Kapitel 5.2 die Schlussfolgerungen für das Vertrauensmanagement zusammen und geht im Kapitel 5.3 auf die Stärken und Limitationen der vorliegenden Arbeit ein. Abgeschlossen wird diese Dissertation im Kapitel 5.4 mit einem Ausblick zu möglichen weiteren spannenden Forschungsfeldern im Bereich der Datenpreisgabe und Vertrauen im Internet sowie einem Blick in die Zukunft.

5.1 Schlussfolgerungen für die Vertrauensforschung

Im ersten Kapitel 5.1.1 werden die zentralen theoretischen Erkenntnisse dieser Dissertation für die wissenschaftliche Gemeinschaft zusammengefasst. Das Kapitel 5.1.2 widmet sich zusammenfassend den empirischen Erkenntnissen dieser Dissertation und das Kapitel 5.1.3 stellt weitere Erkenntnisse aus der Theorie und der Empirie vor.

5.1.1 Theoretische Erkenntnisse

Diese Dissertation hat in einer ausführlichen Literaturrecherche den aktuellen Stand der Forschung zu den drei Themen persönliche Daten, Privacy und Vertrauen im Internet aufgearbeitet. Im Folgenden werden die zentralen Erkenntnisse der Literaturrecherche zusammengefasst, miteinander in Verbindung gebracht und zum Schluss in der Abbildung 88 übersichtlich dargestellt.

Das neue Internet hat zu einer fundamentalen Verschiebung hin zu einer nutzer- und kundenzentrierten Welt geführt, in der Beziehungsaufbau und -pflege zur Kernaufgabe der Online-Anbieter werden (Culnan, 2000; Osterwalder & Pigneur, 2010). Diese Investition in Beziehungen setzt die Kenntnis der persönlichen Vorlieben und Bedürfnisse der Kunden voraus, welche mittels ausführlicher Kundenprofile eruiert werden (Chellappa & Sin, 2005; Miyazaki & Fernandez, 2000). Anbieter sind demnach ökonomisch motiviert, immer mehr über ihre Nutzer zu erfahren (Krasnova et al., 2010). Algorithmen machen es möglich, von vergangenem Nutzerverhalten auf die Zukunft zu schliessen und personalisierte Konsumvorschläge zu machen (Meckel, 2011; Chellappa & Sin, 2005). Persönliche Daten sind im Internet zu einem nachgefragten Gut avanciert und können als neue Währung angesehen werden, welche im Rahmen einer Transaktion getauscht und gehandelt werden. Besonders bei personalisierten Geschäftsmodellen sind persönliche Daten als kritischer Erfolgsfaktor zu betrachten (Montgomery & Smith, 2009; Chellappa & Sin, 2005). Detailliert werden die vier übergeordneten Geschäftsmodelle Online-Information, Online-Shopping, Online-Banking und soziale Netzwerke betrachtet (Timmers, 1998; 2000). Eine zentrale Erkenntnis ist, dass die Bereitschaft der Nutzer, einem Transaktionspartner persönliche Daten zur Verfügung zu stellen, eine notwendige Grundlage für jede Art von Online-Transaktion ist (Culnan & Armstrong, 1999; Milne & Boza, 1999; Eastlick et al., 2006), denn bei jedem Schritt im Internet geben wir persönliche Daten von uns preis (Rust et al., 2002).

Privacy gewinnt durch die Möglichkeiten der Offenlegung und Vernetzung immer mehr an Bedeutung (Rust et al., 2002). Der Nutzer muss bei jeder Transaktion aufs Neue einschätzen, ob das Reziprozitätsverhältnis der geforderten Daten gegenüber dem versprochenen Nutzen stimmt (Rust et al., 2009). Die Nutzer verlangen Kontrolle über die Sammlung, Verbreitung und den Gebrauch ihrer persönlichen Daten (Goodwin, 1991; Milne & Boza, 1999; Phelps et al., 2000; Lanier & Saini, 2008). Die Anliegen der Nutzer bezüglich Privacy im Internet können in die drei Kategorien Monitoring und Tracking, Verbreitung und Veröffentlichung sowie in Aggregation und Analyse eingeteilt werden (Nissenbaum, 2009). Da die Handhabung der eigenen Privacy im Umfeld des Internets schwierig ist, haben die Nutzer Strategien zum Schutz der Privacy entwickelt; dazu gehören eine gezielte Informationssuche, Verschleierungspraktiken, das Anpassen der Privacy-Einstellungen und das bewusste Ausüben seiner Rechte (Youn, 2009; Milne & Rohm, 2000; Milne & Culnan, 2004; Marvick et al., 2010). Der Internetnutzer muss ein Weg finden, seine Privacy im Netz

zu wahren und dennoch an Transaktionen teilnehmen zu können. Damit er dies kann, muss er dem Anbieter vertrauen. Unternehmen können entweder versuchen, die Privacybedenken der Nutzer zu reduzieren, oder sie können versuchen, Vertrauen aufzubauen (Milne & Boza, 1999; Culnan & Armstrong, 1999).

Fehlendes Vertrauen wird als Barriere betrachtet, welche Nutzer von Online-Transaktionen abhält (Urban et al., 2009). Das Vertrauen setzt sich aus den Komponenten Kompetenz, Ehrlichkeit sowie Wohlwollen zusammen (Casalo et al., 2008; Belanger et al., 2002; Lee & Turban, 2001; Urban et al., 2009) und ist situationsabhängig, informationsquellenabhängig, erfahrungsabhängig und persönlichkeitsabhängig (Olson & Olson, 2000; Urban et al., 2009; Rotter 1967). In der Literatur wurden vier Kernelemente von Vertrauen identifiziert, die Erwartungen, die Risikoübernahme, der Kontrollverzicht sowie die Zukunftsausrichtung (Rotter, 1967; Currall & Judge, 1995; Mayer et al., 1995; Schlenker et al., 1973). Vertrauen wird als mehrdimensionales Konstrukt betrachtet, welches aus den Teilbereichen Vertrauensneigung, Vertrauen in die Institution und Vertrauen in den Anbieter besteht (McKnight et al., 1998; 2002a). Insbesondere wenn soziale Situationen von Risiko, Unsicherheit und wechselseitiger Abhängigkeit geprägt sind, gewinnt Vertrauen an Bedeutung (Grabner-Kräuter & Kaluscha, 2003; McKnight & Chervany, 2002). Dies ist insbesondere im Online-Umfeld der Fall, da das Vertrauensobjekt eine Website darstellt (Nissenbaum, 2001). Vertrauen wird dann generiert, wenn der Nutzer positive Eindrücke der Webpräsenz eines Transaktionspartners gesammelt hat und deshalb bereit ist, ein bestimmtes Mass möglicher Enttäuschungen in der Transaktion mit dem Geschäftspartner zu akzeptieren (Urban et al., 2009). Deshalb wird in dieser Dissertation von Vertrauen gesprochen, wenn Nutzer bereit sind, dem Anbieter eines Online-Geschäftsmodells für eine versprochene Leistung persönliche Daten im Internet zu überlassen. Die Beurteilung der Vertrauenswürdigkeit eines Transaktionspartners nehmen Nutzer anhand von Eigenschaften und Eindrücken des Online-Auftritts eines Anbieters vor (Friedman et al., 2000; Jarvenpaa et al., 2000). Die wichtigsten Vertrauensfaktoren im Online-Umfeld sind Reziprozität, Nutzerkontrolle, Kommunikation, Marke, Reputation, Siegel und Zertifikate, Nutzerratings, Design, Technik, Sicherheit, Realweltbezug und Kundenservice. Vertrauen verändert sich über die Zeit, je nach Situation, Information oder Erfahrung des Nutzers (Olson & Olson, 2000), Vertrauen kann demnach Auslöser, aber ebenso Resultat von Transaktionen sein (Rousseau et al., 1998). Die Vertrauensbildung kann in drei Phasen eingeteilt werden: die Phasen des Vertrauensaufbaus, des Erhalts und des Verlustes (Rousseau et al.,

1998). Die Absicht, einem Anbieter in Zukunft zu vertrauen, beinhaltet die Bereitschaft, verwundbar zu sein oder ein Risiko einzugehen (Euijin & Tadisina, 2007; Schlosser et al., 1993).

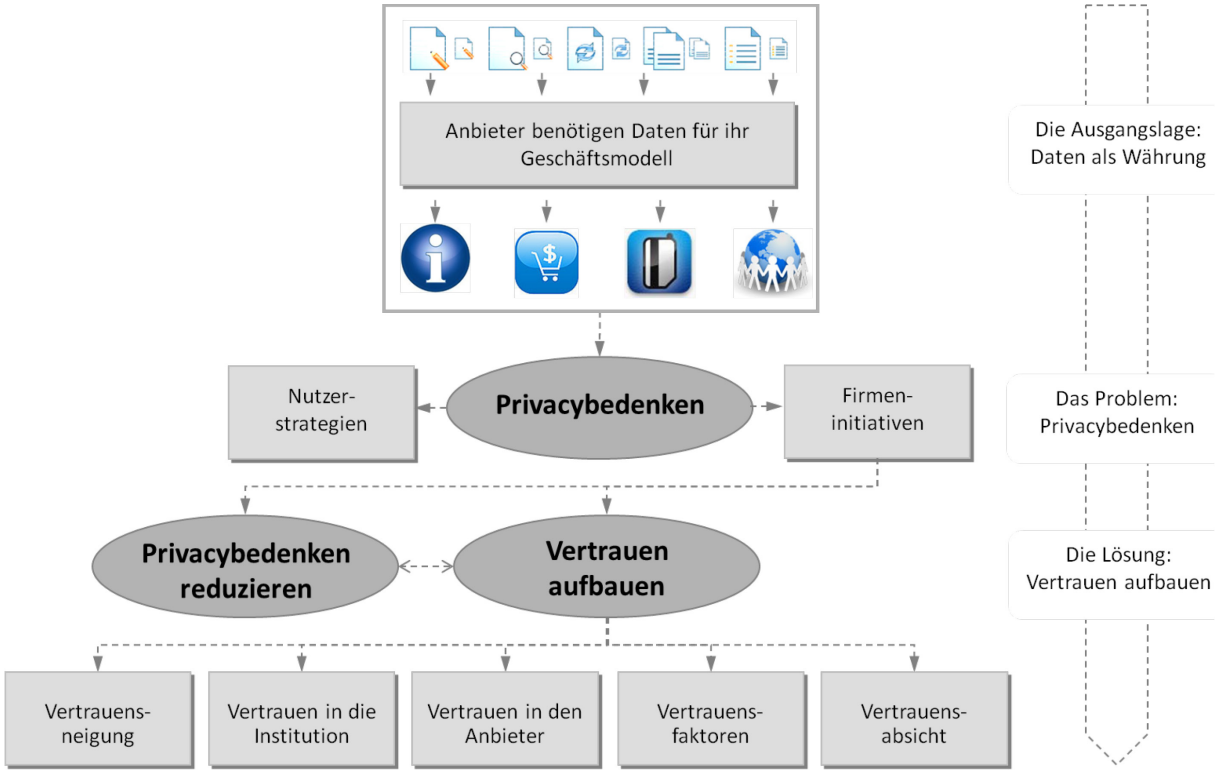


Abbildung 88: Zusammenfassung der theoretischen Erkenntnisse (eigene Darstellung)

Durch die ausführliche Aufarbeitung der relevanten Literatur in diesen drei Teilbereichen wurde festgestellt, dass Vertrauen selten als dynamischer Prozess betrachtet wird und es zwar theoretisch als Persönlichkeitsmerkmal definiert wird, dies bei den wissenschaftlichen Untersuchungen aber oft ausser Acht gelassen wurde. Der Autorin sind keine Studien bekannt, welche untersuchen, ob unterschiedliche Vertrauenstypen im Internet existieren, auf welche Faktoren diese während einer Transaktion achten und ob diese unterschiedliche Vertrauensabsichten aufweisen. Dieser Forschungslücke widmete sich diese Dissertation.

Die zentralen Erkenntnisse der empirischen Forschung dieser Arbeit für die wissenschaftliche Gemeinschaft werden im nächsten Kapitel 5.1.2 zusammengefasst.

5.1.2 Empirische Erkenntnisse

Die im vorhergehenden Kapitel erwähnte Forschungslücke wurde anhand dreier Forschungsfragen geschlossen. (1) „Existieren bei Internetnutzern unterschiedliche Vertrauenstypen?“ Je nach Charaktereigenschaft, Situation, Erfahrung und Information haben Menschen unterschiedliches Vorschussvertrauen und steigen anders in Situationen ein. Diese Dissertation konnte anhand der Faktoren Vertrauen in den Anbieter, Vertrauensneigung und Vertrauen in die Institution mittels Clusteranalyse drei signifikant unterschiedliche Vertrauenstypen differenzieren. Die Interpretationen erfolgten darüber hinaus anhand demografischer Unterscheidungsmerkmale sowie der Internetnutzung. (2) „Sind während einer Transaktion im Internet für die unterschiedlichen Vertrauenstypen dieselben Vertrauensfaktoren relevant?“ Im Internet existieren drei Vertrauenstypen, welche während einer Transaktion auf unterschiedliche vertrauensfördernde Faktoren achten. Diese Erkenntnis wurde aufgrund von Faktorenanalysen und Mittelwertvergleichen gewonnen. (3) „Unterscheiden sich die Vertrauenstypen in Bezug auf ihre Vertrauensabsichten?“ Die dritte Erkenntnis dieser Dissertation ist, dass sich die zukünftigen Verhaltensweisen pro Vertrauenstyp nicht signifikant voneinander unterscheiden: Für alle Vertrauenstypen ist Vertrauen auch das Resultat vorangegangener Transaktionen. Diese Erkenntnis wurde aufgrund eines Mittelwertvergleiches gewonnen. Die zentralen empirischen Erkenntnisse pro Vertrauenstyp werden im Folgenden kurz zusammengefasst und in Abbildung 89 grafisch zusammengestellt:

.

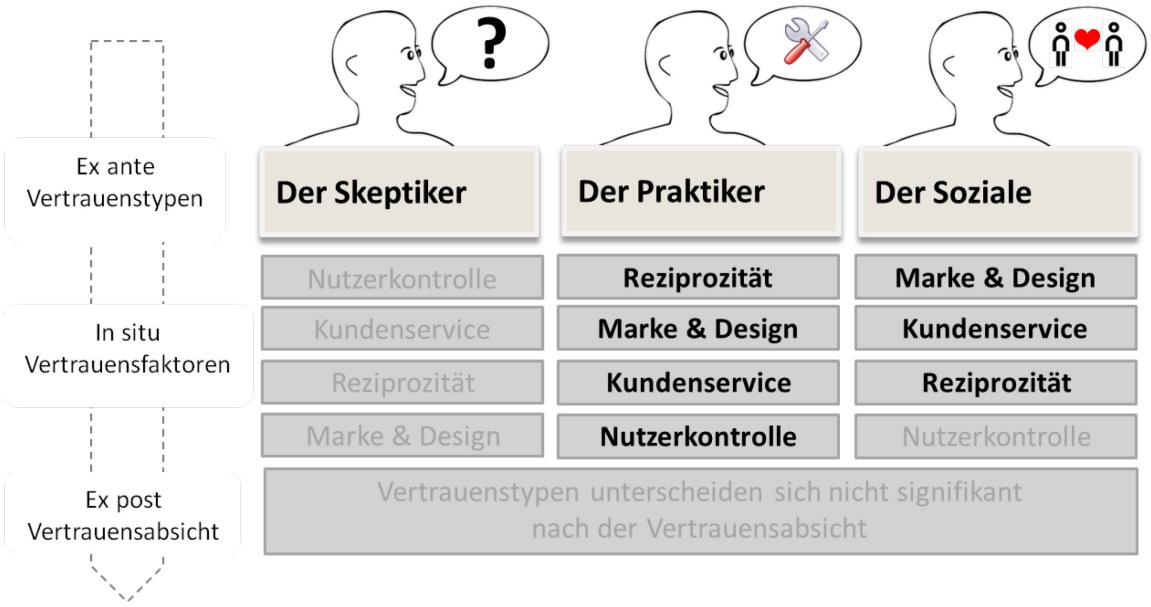


Abbildung 89: Zusammenfassung der empirischen Erkenntnisse (eigene Darstellung)

Der **Skeptiker** hat geringes Vertrauen in den Anbieter, ist tendenziell kritisch gegenüber anderen Menschen eingestellt und weist wenig Vertrauen gegenüber der Institution Internet auf. Der eher jüngere Digital Native ist besonders oft auf sozialen Netzwerkseiten und Community-Plattformen anzutreffen und er geht mit seinen persönlichen Daten im Netz offen um. Er unterscheidet nicht zwischen Offline- und Online-Welt, sondern hat ein sehr entspanntes Verhältnis gegenüber dem Internet. Er ist im Vergleich zu den anderen Typen gut gebildet oder noch immer in Ausbildung. Der Skeptiker achtet während einer Transaktion im Netz am wenigsten stark auf vertrauensfördernde Faktoren.

Der **Praktiker** hat vergleichsweise grosses Vertrauen in den Anbieter und das Internet, vertraut dafür aber anderen Menschen eher weniger. Obwohl der Praktiker der älteste Vertrauenstyp ist und zu den Digital Immigrants gehört, scheint er sich im Internet sicher zu fühlen. Der Praktiker verfügt über einen Real- oder Berufsschulabschluss und nutzt auffällig oft Online-Games, kauft online ein und tätigt seine Bankgeschäfte per Online-Banking. Er nutzt eher konservative Geschäftsmodelle und handhabt seine persönlichen Daten im Netz restriktiv. Der Praktiker achtet auf alle vier Vertrauensfaktoren, insbesondere auf das Reziprozitätsverhältnis, auf die Marke und das Design eines Anbieters, auf den Kundenservice sowie auf Kontroll-

möglichkeiten über seine Daten. Er bildet sich gründlich eine Meinung und lässt die Vertrauensindikatoren auf sich wirken, bevor er eine Entscheidung fällt.

Der **Soziale** vertraut den Menschen und dem Anbieter, dem Internet als Institution vertraut er aber tendenziell nicht. Sein Fokus liegt auf Menschen und Beziehungen zu Menschen in der realen Welt. Er sticht in dieser Umfrage nirgends hervor, sondern fällt vielmehr durch seine häufige Mittelfeldposition auf. Der Soziale achtet während einer Transaktion besonders auf ein angemessenes Reziprozitätsverhältnis, auf die Marke und das Design eines Anbieters sowie auf den Kundenservice.

Im folgenden Kapitel 5.1.3 werden weitere zentrale Erkenntnisse aus der Theorie und der Empirie diskutiert.

5.1.3 Weitere Erkenntnisse aus Theorie und Empirie

Im Literaturüberblick wurden verschiedene Studien und deren Ergebnisse zitiert und diskutiert. Einzelne zentrale Erkenntnisse dieser Studien werden in diesem Kapitel mit den Erkenntnissen dieser Dissertation verglichen und verbunden.

Alter: Die Forscher Mesch und Beker (2010) stellen fest, dass das Alter eine zentrale Rolle bei der Offenlegung der Daten im Internet hat. Ihre Forschung ergab, dass jüngere Nutzer tendenziell weniger persönliche Informationen von sich preisgeben. Andererseits sind sich Wissenschaftler darin einig, dass sich besonders junge Menschen zu wenig Gedanken über die Privatheit ihrer Daten im Internet machen (Palfrey & Gasser, 2008; Edwards & Brown, 2009; Sheehan & Hoy, 2000). Der Skeptiker ist der jüngste Vertrauenstyp und er weist die niedrigste „Keine Antwort"-Rate auf. Diese Studie kommt zu dem Schluss, dass mit sinkendem Alter der Nutzer die Bereitschaft steigt, mehr Daten von sich preiszugeben. Die Ergebnisse von Mesch und Beker (2010) können in dieser Hinsicht nicht bestätigt werden, dafür bestätigt sich aber die Tendenz, dass jüngere Nutzer eher weniger auf ihre Privacy im Netz achten.

Bildung und Nutzerkontrolle: Culnan (1995) konnte aufzeigen, dass besonders junge und ärmere Personen mit geringerer Bildung wenige Kenntnisse zum Schutz ihrer Privacy im Internet mitbringen. Phelps et al. (2000) bestätigten diese Erkenntnisse in ihrer Studie, indem sie aufzeigten, dass 51 % der Personen mit einem Universitätsabschluss oder einer Berufsschule Bedenken äusserten, wie Unternehmen mit ihren privaten Daten umgehen. Diese Erkenntnisse können anhand des Faktors

Nutzerkontrolle verglichen werden. Der Skeptiker ist gut gebildet, achtet aber im Vergleich eher weniger auf den Faktor Nutzerkontrolle. Der Praktiker hat den niedrigsten Bildungsstand, achtet aber klar darauf, wer die Kontrolle über seine persönlichen Daten ausübt. Der Soziale liegt bei der Bildung im Mittelfeld und achtet auch nicht stark auf die Nutzerkontrolle. Die Ergebnisse von Culnan (1995) sowie Phelps et al. (2000) können durch diese Studie nicht bestätigt werden.

Privacy-Paradox: Wenn private Daten trotz Privacybedenken im Internet offengelegt werden, spricht man vom Privacy-Paradox, wie im Kapitel 2.2.2.2 dargelegt wurde (Barnes, 2006). Das tatsächliche Verhalten eines Internetnutzers stimmt demnach oftmals nicht mit der Aussage überein, seine Privacy schützen zu wollen (Acquisti & Gross, 2006). Der Skeptiker hat in der Online-Umfrage angegeben, dass er es problematisch findet, dem Anbieter persönliche Daten zu überlassen, und hat gleichzeitig am häufigsten alle Fragen der Umfrage beantwortet. Darüber hinaus nutzt der Skeptiker mit Abstand am häufigsten soziale Netzwerke und Online-Communitys, bei welchen viele persönliche Daten zur Verfügung gestellt werden müssen. Eine Erklärung dafür könnte sein, dass diese Nerzwerke als geschlossenes System und somit als privat betrachtet werden (Jones, Johnson-Yale, Millermaier & Pérez, 2009). Auch beim Praktiker sind Aussage und Verhalten zur Datenpreisgabe nicht kongruent. Der Praktiker findet es unproblematisch, dem gewählten Anbieter persönliche Daten zu überlassen, gleichzeitig weist er die höchste „Keine Antwort"-Rate auf. Der Praktiker geht überaus restriktiv mit seinen persönlichen Daten um, obwohl er keine Privacybedenken hat. Beim Praktiker ist demnach das Gegenteil des Privacy-Paradoxes zu beobachten. Bei Internetnutzern, die dem sozialen Typ angehören, stimmen Aussagen über die Datenhandhabung und tatsächliches Verhalten überein. Das von Barnes (2006) beobachtete Privacy-Paradox kann somit nur beim Skeptiker eindeutig bestätigt werden.

Geschlecht: Sheehan (1999) hat in seiner Studie untersucht, wie sich das Geschlecht auf den Umgang mit Privacy im Internet auswirkt. Er fand heraus, dass Frauen im Vergleich zu den Männern im Allgemeinen mehr Bedenken darüber haben, welche Auswirkung die Sammlung von Daten auf ihre Privacy haben kann. Um diese Aussage zu überprüfen, vergleichen wir die Datenhandhabung des Skeptikers (eher männlich) mit derjenigen des Sozialen (eher weiblich). Der Skeptiker stuft das Überlassen von privaten Daten an den Anbieter als problematisch ein, der Soziale sieht darin kein Kernproblem. Dass Frauen mehr Bedenken hinsichtlich der Sammlung und Aggregation ihrer persönlichen Daten haben, kann mit dieser Studie nicht

bestätigt werden. Es muss aber darauf hingewiesen werden, dass dem Geschlecht in dieser Studie keine signifikante Trennkraft zukam.

Die Studie von Dommeyer und Gross (2003) stellte fest, dass Männer, insbesondere junge Männer, bewusster Strategien erkennen und anwenden, um persönliche Informationen zurückzuhalten. Diese Studie kann anhand des Skeptikers gemessen werden, der in der Tendenz jung und männlich ist. Beim Skeptiker wurde das Privacy-Paradox identifiziert (tatsächliches Verhalten stimmt nicht mit der Aussage überein), was darauf hindeutet, dass die Studienergebnisse von Dommeyer und Gross (2003) nicht auf den Skeptiker übertragbar sind.

Internetnutzung und Datenpreisgabe: In ihrer Studie konnten Mesch und Beker (2010) nachweisen, dass ein positiver Zusammenhang zwischen Internetnutzung und Offenlegung persönlicher Informationen besteht. Je intensiver das Internet genutzt wird, desto eher ist die Person bereit, Daten preiszugeben. In dieser Studie nutzt der Praktiker das Internet am häufigsten und er weist gleichzeitig auch die höchste „Keine Antwort"-Rate auf. Demnach kann der beobachtete positive Zusammenhang zwischen der Offenlegung von Information und der Internetnutzung nicht bestätigt werden.

Vertrauen in die Institution und Nutzung von Online-Banking: Im Theoriekapitel Vertrauen (Kapitel 2.3.1.3) wurde darauf hingewiesen, dass sich nur Nutzer mit hohem Institutionsvertrauen beim Online-Banking registrieren (Kim & Prabhakar, 2002). Im Kapitel 2.2.3.1 haben wir gesehen, dass insbesondere Finanzdaten als sensible Informationen eingestuft werden und dass es deshalb Sinn ergibt, dass nur Personen mit hohem Institutionsvertrauen ihre Banktransaktionen online abwickeln. Diese Studie kann die Ergebnisse von Kim und Prabhakar (2002) für alle Vertrauenstypen bestätigen: Der Praktiker hat hohes Vertrauen in die Institution Internet und nutzt am meisten Online-Banking-Dienstleistungen. Der Skeptiker hat mässiges Vertrauen in die Institution und befindet sich bei der Nutzung von Online-Banking im Mittelfeld. Der Soziale hat im Vergleich eher wenig Vertrauen in die Institution und nutzt am wenigsten Online-Banking-Dienstleistungen.

Im nächsten Kapitel werden die Schlussfolgerungen für das Vertrauensmanagement im Detail betrachtet.

5.2 Schlussfolgerungen für das Vertrauensmanagement

Im folgenden Kapitel 5.2.1 wird auf die zentralen Erkenntnisse des Vertrauensmanagements dieser Dissertation für Anbieter von Online-Geschäftsmodellen eingegangen und im Kapitel 5.2.2 werden konkrete Handlungsempfehlungen pro Vertrauenstyp abgeleitet.

5.2.1 Zentrale Erkenntnisse des Vertrauensmanagements für die Praxis

Das Internet ist geprägt von unsicheren und risikoreichen Situationen für die Nutzer. Diese Arbeit verdeutlicht, dass das Vertrauen der Nutzer eine Schlüsselrolle spielt, um Transaktionen im Internet zu tätigen. Ist das Vertrauen nicht vorhanden, kann das Wertschöpfungspotenzial des Internets für Wirtschaft, Kultur und Gesellschaft nicht voll ausgeschöpft werden. Dieses Kapitel leitet die zehn wichtigsten Erkenntnisse dieser Dissertation über das Vertrauensmanagement für die Praxis ab, wie in Abbildung 90 zusammengefasst.

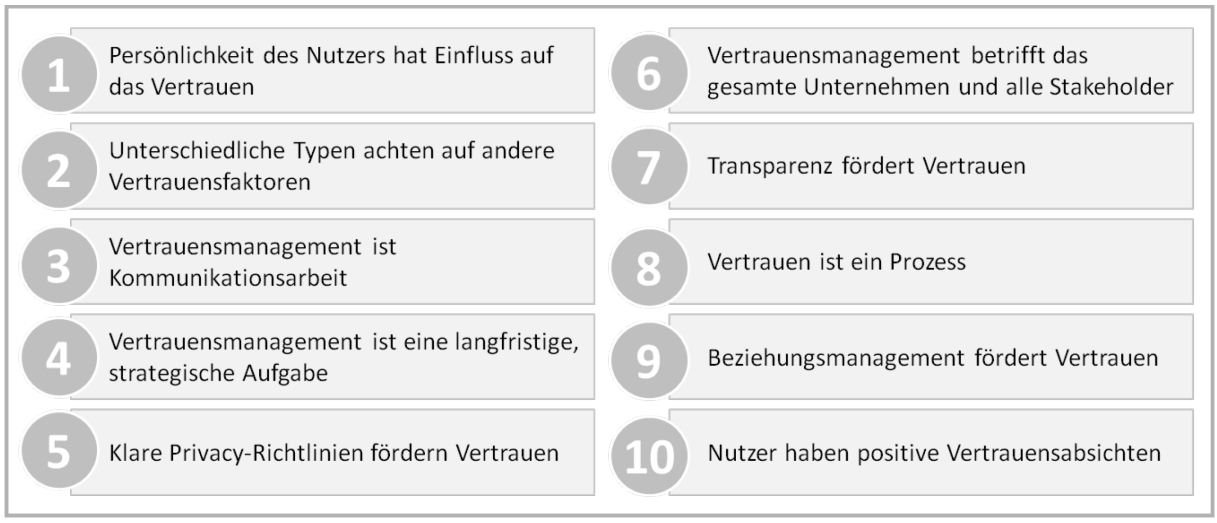


Abbildung 90: Zentrale Erkenntnisse des Vertrauensmanagements für die Praxis (eigene Darstellung)

1) Persönlichkeit des Nutzers hat Einfluss auf das Vertrauen

Eine zentrale Erkenntnis dieser Dissertation ist, dass Risiken von jedem Nutzer individuell unterschiedlich aufgenommen werden und dass Nutzer unterschiedlich schnell und aus anderen Beweggründen heraus Vertrauen aufbauen. Vertrauensforscher gehen davon aus, dass Vertrauen auf sozialen Beziehungen, Gruppenzugehörigkeit und geteilten Werten basiert. Demnach können das Vorschussvertrauen und die Bildung von Vertrauen in verschiedenen geografischen und kulturellen Regionen stark variieren. Demografische Variablen, Bildungsstand oder das gewählte Online-Geschäftsmodell beeinflussen die Wahrnehmung von Risiken und somit die Bereitschaft, persönliche Daten zur Verfügung zu stellen, um an Transaktionen im Internet teilzunehmen. Darüber hinaus sind Individuen je nach persönlichen Charakterzügen, Erfahrungen oder psychologischen Merkmalen mehr oder weniger in der Lage zu vertrauen. Deshalb ist es eminent wichtig, dass Online-Anbieter wissen, wer ihre Zielgruppe ist, um gezielt Vertrauen aufzubauen und zu pflegen.

2) Unterschiedliche Typen achten auf andere Vertrauensfaktoren

Die Auswertungen dieser Dissertation zeigen, dass sich die Vertrauensfaktoren signifikant nach Typ unterscheiden (siehe Kapitel 3.2.2), und belegen, dass unterschiedliche Typen auf andere Vertrauensfaktoren achten. Jeder Mensch bringt ein gewisses Mass an Vertrauen und unterschiedliche Erfahrungen in eine Situation hinein. Vertrauen ist aber auch abhängig von der Transaktion selbst sowie dem jeweiligen Online-Geschäftsmodell. Dass Unternehmen auf diesen Teil des Vertrauens durch die Vertrauensfaktoren Einfluss nehmen können, zeigt diese Dissertation. Je nach Vertrauenstyp müssen unterschiedliche Faktoren zur Vertrauensbildung in den Vordergrund gestellt und kommuniziert werden. Konkrete Handlungsempfehlungen für Anbieter von Online-Geschäftsmodellen pro Vertrauenstyp werden im Kapitel 5.2.2 im Detail vorgestellt.

3) Vertrauensmanagement ist Kommunikationsarbeit

Diese Dissertation konnte aufzeigen, dass Vertrauensmanagement Kommunikationsarbeit ist, weil Marke und Design einen starken Einfluss auf die Wahrnehmung des Nutzervertrauens haben. Das Managen der Unternehmensreputation und des Images ist seit Jahren zentraler Bestandteil der Kommunikationsarbeit (Argenti, 1998). Das Kommunikationsmanagement muss daneben auch zum Ziel haben, das

Vertrauen der Nutzer zu pflegen und zu fördern sowie das der Nichtnutzer zu gewinnen. Die Vertrauensbildung muss als eine kommunikative Aufgabe betrachtet werden, denn alle Informationen, welche für eine mögliche Transaktion benötigt werden, müssen über die Homepage kommuniziert werden. Die Sozialen Medien eröffnen Anbietern enorm viele Möglichkeiten, den Nutzer mit relevanten Informationen zu versorgen und mit ihm zu interagieren. Dabei ist wichtig, dass die Verantwortlichen mit den Gepflogenheiten, der Philosophie und der Sprache der einzelnen Portale vertraut sind. Der Einsatz der Plattformen muss aufeinander abgestimmt sein. Es kann nicht Ziel sein, flächendeckend in den Sozialen Medien präsent zu sein, sondern vielmehr sollten sich Anbieter auf einzelne, ausgewählte Portale konzentrieren. Gleichzeitig zeigen die Auswertungen, dass je nach Vertrauenstyp die herkömmlichen Kommunikationskanäle nicht vernachlässigt werden sollten. Der Bezug zur realen Welt kann vertrauensfördernd wirken und zudem Nicht-Internetnutzer beim Schritt ins Netz unterstützen. Reichen dem Nutzer die Informationen im Netz nicht aus, ist er unsicher oder verärgert und bricht die Transaktion ab. Deshalb muss immer die Möglichkeit bestehen, den Kundenservice des Unternehmens über ein Callcenter, über E-Mails oder per Post zu kontaktieren. Eine wichtige Erkenntnis dieser Arbeit ist, dass das Unternehmen konsistent in Wort, Tat und Verhalten sein muss.

4) Vertrauensmanagement ist eine langfristige, strategische Aufgabe

Das Management von Vertrauen ist eine strategische und somit langfristige Aufgabe. Vertrauen bei den Nutzern aufzubauen, muss eines der zentralen strategischen Ziele des Unternehmens sein, denn ohne Vertrauen tätigen die Nutzer keine Transaktion im Internet, wie diese Dissertation aufzeigen konnte. Vertrauen ist ein Prozess und wird über die Zeit hinweg gefestigt und bestätigt. Ein einzelner negativer Vorfall kann das Vertrauen vollständig zerstören, daher muss im Voraus ein klares Krisenkommunikationskonzept ausformuliert werden. Wichtig ist, dass sich Anbieter nicht kurzfristig von Shitstorms, Datenschutzskandalen oder medialer Aufmerksamkeit vom Weg abbringen lassen. Änderungen bei den Richtlinien, im Webauftritt oder im Design sollten nicht im Wochenrhythmus vorgenommen werden. Die Auswertungen zeigen, dass Kontinuität auch im Internet ein wichtiger Wert ist und Nutzer auf Wiedererkennungsmerkmale achten. Deshalb sollten radikale Änderungen im Vorfeld offen kommuniziert werden und von verständlichen, zusammenfassenden Informationsschreiben begleitet werden.

5) Klare Privacy-Richtlinien fördern Vertrauen

In den letzten Jahren ist zu beobachten, dass dem Thema Privacy im Internet vermehrt mediale Aufmerksamkeit zuteilwird. Auch diese Dissertation unterstreicht die Wichtigkeit von Privacy: Anbieter von Online-Geschäftsmodellen können über die Privacy-Richtlinien Vertrauen generieren, weil sich Nutzer bei der Preisgabe ihrer persönlichen Daten auf die Privacy-Richtlinien stützen. Persönliche Daten in einer technologiebasierten Umgebung zu veröffentlichen, bedeutet für Nutzer Unsicherheit. Deshalb gehört es zu den wesentlichen Elementen der Vertrauenspflege, die Datenschutzrichtlinien und somit die Rechte und Pflichten der Nutzer umfassend, aber verständlich zu kommunizieren und Kunden auf die implementierten Sicherheitsmassnahmen aufmerksam zu machen. Nur wenn die Datenschutzrichtlinien des Unternehmens lesbar und verständlich sind, können Nutzer ihre Rechte auch ausüben. Lesbarkeit wird anhand des Schwierigkeitsgrades sowie der Nachvollziehbarkeit gemessen (Flesch, 1949). Es nützt nichts, wenn Unternehmen besonders detailliert ihre Datenschutzbestimmungen publizieren, sondern es sollte auf die jeweiligen Bedenken eingegangen werden und erklärt werden, unter welchen Umständen die Kunden welche Rechte haben und wie diese ausgeübt werden können. Unternehmen müssen ihre Datenschutzrichtlinien überdenken und die Richtlinien transparenter, einfacher und verständlicher formulieren. Untersuchungen ergaben jedoch, dass viele Richtlinien weder transparent noch für den Leser verständlich formuliert sind (Pollach, 2005). Zum Beispiel benutzen Unternehmen oft komplizierte und unverständliche Fachbegriffe, um Privacy relevanten Themen auszuweichen. Eine Längsschnittstudie von Milne et al. (2006), in der 312 Datenschutzrichtlinien untersucht wurden, ergab, dass die Lesbarkeit, aber auch die Länge der untersuchten Richtlinien zugenommen haben. Die Richtlinien waren so formuliert, dass der Grossteil der Bevölkerung dem Text nicht folgen konnte. Ausserdem werden Ankündigungen über Änderungen der Privacy-Richtlinien meistens als eine Verschärfung zu Ungunsten des Nutzers wahrgenommen. Betrachtet man die Entwicklung der Privacy-Statements von Facebook in den Jahren 2005 bis 2012 (Abbildung 91), wird ersichtlich, dass diese jedes Jahr umfassender und somit für den Nutzer unübersichtlicher werden (Gates, 2010).

Abbildung 91: Anzahl der Wörter der Privacy-Statements bei Facebook (eigene Darstellung in Anlehnung an Gates, 2010)

Jede Firma kann ihre eigenen Privacy Normen im Rahmen des gesetzlich Möglichen definieren und der Nutzer muss diese akzeptieren, wenn er partizipieren möchte. Welcher Nutzer liest eine aus 6'814 Wörter bestehende, kompliziert formulierte Richtlinie, bevor er sich bei einem sozialen Netzwerk anmeldet? Es erstaunt nicht, dass die meisten Konsumenten die Datenschutzrichtlinien nicht lesen und so auch nicht wissen, was ihre Rechte sind und diese nicht bewusst ausüben können (Milne et al., 2004). Unkenntnis löst bei den Nutzern Unsicherheit sowie das Gefühl eines Kontrollverlustes aus. Online-Anbieter sollten die Bedürfnisse und Erwartungen ihrer Nutzer bezüglich der Datensicherheit kennen und diese möglichst in ihre Privacy-Richtlinien eingliedern. Die Kommunikation von verständlichen und transparenten Datenschutzrichtlinien ist ein wichtiger Wegbereiter für einen effektiven Schutz der Privacy und den Aufbau von Vertrauen durch Unternehmen.

6) Vertrauensmanagement betrifft das gesamte Unternehmen und alle Stakeholder

In einem offenen Netzwerk wie dem Internet kann nie nur eine spezifische Anspruchsgruppe betrachtet werden, sondern es handelt sich immer um ein Geflecht aus Beziehungen unterschiedlicher Personen und Organisationen. Beim Managen von Vertrauen darf deshalb nicht nur auf den Nutzer selbst fokussiert werden, sondern es muss ein ganzes Netzwerk von Anspruchsgruppen beachtet und integriert werden, welche sich gegenseitig beeinflussen. Anbieter von Online-Geschäftsmodellen müssen diese Interdependenzen erkennen und versuchen, diese für sich zu nutzen. Für die Kommunikation von Vertrauen spielen insbesondere die Mitarbeiter als Schnittstelle zum Nutzer eine zentrale Rolle. Mitarbeiter tragen die Botschaften des Unternehmens weiter und dienen als Verstärker. Das Ziel, ein vertrauenswürdiger Anbieter zu sein, muss vom gesamten Unternehmen mitgetragen werden und auch im internen Umgang gelebt werden, damit glaubwürdig nach aussen kommuniziert werden kann. Ebenso zentral ist ein gegenseitiges Vertrauensverhältnis mit den Lieferanten, damit die Wertschöpfungskette optimal funktioniert. Weiter spielt die Wahrnehmung des Unternehmens durch potenzielle Nutzer, Nichtnutzer, mögliche Gegner oder Drittorganisationen eine wichtige Rolle, da diese das Image und die Reputation des Unternehmens prägen. Aussagen und Empfehlungen von Drittparteien über ein Unternehmen und dessen Produkte sind viel glaubwürdiger als Werbebotschaften des Unternehmens selbst.

7) Transparenz fördert Vertrauen

Die Offenlegung von Informationen unterstützt die Wahrnehmung der Nutzer, dass Unternehmen als vertrauenswürdig eingestuft werden können. Diese Dissertation zeigt auf, dass Nutzer auf faire Informationspraktiken achten und ein gewisses Mass an Kontrolle über den Prozess benötigen, um dem Anbieter ihr Vertrauen entgegenbringen zu können. Die Schaffung von Transparenz basiert auf Kommunikationsarbeit und baut Misstrauen gegenüber dem Unternehmen durch Informationen ab, wodurch kein Raum für Gerüchte oder Spekulationen entstehen kann. Darüber hinaus erleichtert Transparenz die Mitbestimmung und die Teilnahme der Nutzer. Eine offene und transparente Informationspolitik führt ausserdem dazu, dass der Konversationspartner im Gegenzug auch mehr Informationen von sich zur Verfügung stellt. Die Auswertungen zeigen, dass Transparenz für den Vertrauensprozess

eminent wichtig ist, da Transparenz dem Nutzer Kontrollmechanismen in die Hand gibt. Ausserdem wird Transparenz als Zeichen der Wertschätzung betrachtetet, als Indiz dafür, dass der Nutzer als zentraler Partner erkannt wird, welcher einen fairen Informationsaustausch verdient.

8) Vertrauen ist ein Prozess

Der Prozess der Vertrauensbildung entsteht nicht erst beim Einloggen ins Internet, sondern Vertrauen bildet sich kontinuierlich über die Zeit. Vertrauen ist ein dynamischer Prozess aus Vorschussvertrauen, Bestätigung oder Vertrauensverlust. Diese Dissertation zeigt auf, dass Vertrauen Auslöser, aber ebenso Resultat von Transaktionen sein kann und dass sich Vertrauen über die Zeit verändert, je nach Situation, Information oder Erfahrung des Nutzers. In Situationen, in denen glaubwürdige und aussagekräftige Informationen über die Vertrauen in Anspruch nehmende Partei unbekannt sind, spielt das mitgebrachte Vorschussvertrauen eine zentrale Rolle. Während der Transaktion achtet der Nutzer auf mögliche Vertrauensindikatoren und nach Durchführung entscheidet sich, ob sich das Vertrauen bestätigt und somit erhalten bleibt oder ob das Vertrauen verloren geht. Unternehmen müssen sich für ein ganzheitliches Vertrauensmanagement in den Nutzer hineinversetzen und den Vertrauensprozess zusammen mit dem Entscheidungsfindungsprozess analysieren.

9) Beziehungsmanagement fördert Vertrauen

Online-Geschäftsmodell-Anbieter müssen von Anfang an in eine vertrauensvolle Beziehung mit dem Nutzer investieren. Das Beziehungsmanagement umfasst alle Stakeholder, im Mittelpunkt steht jedoch der Kunde oder der Nutzer (auch bekannt unter dem Begriff Customer-Relationship-Management, kurz CRM). Ziel des Beziehungsmanagements ist eine hohe Nutzerbindung, Nutzerloyalität und der Aufbau von Vertrauen. Wenn Nutzer dem Anbieter vertrauen, sind sie eher bereit, persönliche Informationen über sich preiszugeben und ermöglichen damit den Aufbau einer Beziehung. Dadurch ist es dem Anbieter möglich, personalisierte Produkte und Dienstleistungen anzubieten, welche auf individuelle Kundenbedürfnisse zugeschnitten sind, wodurch das Vertrauen wie auch die Loyalität zum Anbieter gestärkt und die Beziehung gefestigt wird.

10) Nutzer haben positive Vertrauensabsichten

Diese Studie konnte aufzeigen, dass der Grossteil der Internetnutzer nach einer durchgeführten Transaktion positive Vertrauensabsichten aufweisen. Die Vertrauensabsicht pro Vertrauenstyp unterscheidet sich nicht signifikant, alle waren positiv. Vertrauen Nutzer einem bestimmten Anbieter und haben sie sich für eine Transaktion entschieden, geben sie auch ihre persönlichen Daten preis. Wenn für den Nutzer der Transaktionsablauf stimmig ist und wenn die Transaktion erfolgreich verlaufen ist, wird der Nutzer in Zukunft mit einer hohen Wahrscheinlichkeit die Seite wieder besuchen, ansonsten hätte er den Prozess bereits während der Transaktion abgebrochen. Grund dafür ist, dass nach Durchlaufen des Entscheidungsfindungsprozesses das persönlich empfundene Risiko gegenüber dem Anbieter sinkt und eine erneute Transaktion wahrscheinlicher wird. Die Erkenntnis dieser Dissertation, dass Nutzer nach einer Transaktion tendenziell positive Vertrauensabsichten haben, bedeutet für Anbieter von Online-Geschäftsmodellen, dass insbesondere vor und während des Entscheidungsfindungsprozesses in vertrauensfördernde Massnahmen investiert werden muss.

Im nächsten Kapitel werden konkrete Handlungsempfehlungen für Anbieter von Online-Geschäftsmodellen für die drei unterschiedlichen Vertrauenstypen abgeleitet.

5.2.2 Handlungsempfehlungen für Anbieter von Online-Geschäftsmodellen

Die Handlungsempfehlungen für das Vertrauensmanagement dienen dazu, den Anbietern von Online-Geschäftsmodellen die in dieser Arbeit gewonnen empirischen Erkenntnisse zugänglich zu machen. Diese Studie konnte aufzeigen, dass im Web drei unterschiedliche Vertrauenstypen existieren, welche der Institution Internet, den Online-Anbietern und den Menschen unterschiedlich schnell vertrauen. Interessant ist nun, wie Informationen im Netz für diese unterschiedlichen Nutzer aufbereitet werden sollte. Da sich die Wahrnehmung von Vertrauenswürdigkeit pro Vertrauenstyp signifikant unterscheidet, ergibt es Sinn, auch das Management von Vertrauen pro Vertrauenstyp zu differenzieren. In diesem Kapitel wird diskutiert, welche Massnahmen das Kommunikationsmanagement ergreifen kann, um Vertrauen bei den drei identifizierten Vertrauenstypen zu erzeugen und zu erhalten.

5.2.2.1 Handlungsempfehlungen für den Skeptiker (Vertrauenstyp 1)

Der Skeptiker ist in Bezug auf die Kommunikationsarbeit der anspruchsvollste Vertrauenstyp. Er ist jung, gut gebildet und als Digital Native ist sein Leben mit dem Internet bereits verflochten. Er nutzt überdurchschnittlich oft soziale Netzwerke und Online-Informationen-Anbieter. Er hebt sich im Vergleich ganz klar durch sein äusserst geringes Vertrauen in den Anbieter ab, hat tendenziell kein Vertrauen gegenüber anderen Menschen, dafür aber mässiges Vertrauen in das Internet. Der Skeptiker achtet während einer Transaktion im Internet im Vergleich am wenigsten stark auf die untersuchten Vertrauensfaktoren. Er lässt sich nicht gerne festlegen, ist eher misstrauisch gegenüber dem Anbieter und vertraut nur sehr spezifisch. Er will eigene Entscheidungen fällen und er reagiert negativ bei Beeinflussungsversuchungen, das heisst, er bricht womöglich die Transaktion ab, wenn er das Gefühl hat, nicht mehr frei entscheiden zu können. Er ist ein Einzelkämpfertyp mit einer Tendenz zum Individualisten. Kontrolle und Selbstbestimmtheit sind für ihn zentral.

Anbieter von Online-Geschäftsmodellen, welche den Skeptiker als Zielgruppe anvisieren, sollten insbesondere auf folgende Handlungsempfehlungen zum Aufbau und zur Pflege von Vertrauen (Abbildung 92) achten:

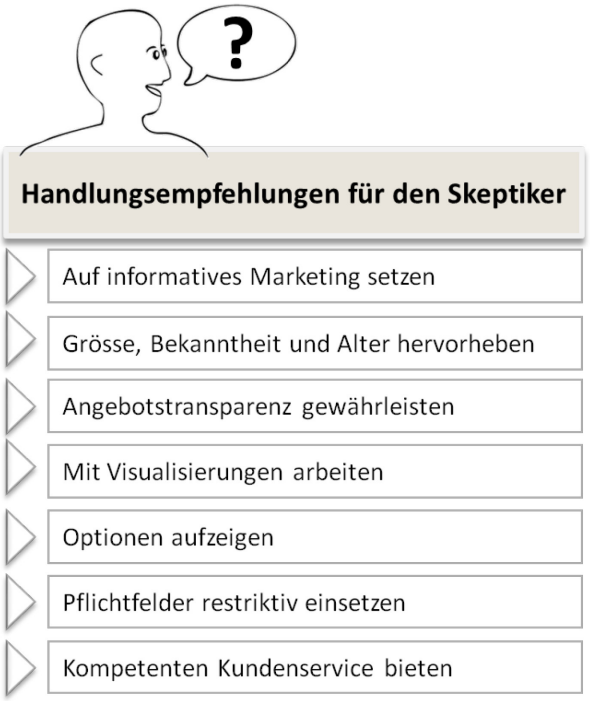


Abbildung 92: Handlungsempfehlungen für den Skeptiker (eigene Darstellung)

Auf informatives Marketing setzen

Anbieter von Online-Geschäftsmodellen sollten den Skeptiker bei der Entscheidungsfindung unterstützen und ihn mit Informationen versorgen, denn Selbstbestimmtheit ist für ihn zentral. Die Auswertungen haben gezeigt, dass der Skeptiker nicht besonders stark auf die Vertrauensfaktoren achtet und dass er frei und unabhängig entscheiden will. Werbung sollte deshalb vor allem aufschlussreich, sachlich und informativ sein, genauso wie die auf der eigenen Homepage zur Verfügung gestellten Informationen. Der Skeptiker reagiert sensibel auf Fremdbestimmung und insbesondere auf direkte Beeinflussung von Anbietern von Online-Geschäftsmodellen. Er weiss, dass Marketing für Online-Anbieter elementar ist, und er schätzt kreative, neue und humorvolle Kampagnen. Auch PR-Texte mit informativem Charakter bevorzugt er, wenn die Intention und der Absender der Botschaft klar erkennbar sind. Er legt viel Wert auf Unabhängigkeit, er möchte stets souverän sein und auch so handeln können. Er nutzt Marketingkampagnen, um sich zu informieren und up to date zu sein, damit er Entscheidungen aufgrund seiner eigenen Recherchen und Erfahrungen treffen kann. Hat er das Gefühl, dass er zu einem Entscheid gedrängt wird, bricht er die Transaktion ab. Der Skeptiker weiss, dass sich gute Web-Applikationen sehr schnell viral verbreiten und aggressive Werbung (wie zum Beispiel blinkende Banner) sind für ihn ein Indiz dafür, dass der Anbieter entweder nicht seriös ist, kein gutes Produkt vertreibt oder noch nicht etabliert ist. In den Augen des Skeptikers verliert ein Anbieter durch solche Praktiken an Vertrauenswürdigkeit. Anbieter von Online-Geschäftsmodellen sollten beim Skeptiker auf aggressive Beeinflussungsversuche verzichten und auf informatives Marketing setzen.

Grösse, Bekanntheit und Alter hervorheben

Anbieter von Online-Geschäftsmodellen sollten sich darauf konzentrieren, Grösse, Bekanntheit oder Alter des Unternehmens in ihrer Kommunikationsarbeit besonders hervorzuheben, denn diese Indikatoren sind für den Skeptiker von zentraler Bedeutung für die Beurteilung der Vertrauenswürdigkeit. Zum Beispiel könnten Anbieter bereits in ihrem Logo auf einen dieser Faktoren hinweisen, einen Verweis darauf bei Suchmaschinen platzieren oder aber auf der Applikationen-Startseite prominent darauf verweisen und Hintergrundinformationen dazu anbieten. Als Digital Native weiss der Skeptiker, dass das Internet sehr schnelllebig und in hohem Masse kompe-

titiv ist. Er hat schon oft gesehen, dass es eine natürliche Selektion über die Zeit gibt und dass sich nur die Besten im Markt etablieren können. Deshalb achtet er darauf, ob der Anbieter bereits eine Weile im Markt existiert und eine konstante Qualität anbietet. Durch Informationen über die Grösse eines Portals zieht der Skeptiker gleichzeitig Schlüsse über das Alter oder die Bekanntheit und vice versa. Er nimmt an, dass Portale organisch exponentiell wachsen und dass je älter ein Portal ist, desto höher die Wahrscheinlichkeit, dass es bekannt ist und eine gewisse Grösse und somit eine gute Angebotsqualität aufweist.

Angebotstransparenz gewährleisten

Die Auswertungen zeigen, dass der Skeptiker genau wissen will, welche Verpflichtungen er eingeht und deshalb ist Transparenz für den Skeptiker von hoher Bedeutung für die Beurteilung der Vertrauenswürdigkeit. Anbieter von Online-Geschäftsmodellen müssen darauf achten, dass sie das Angebot selbst sowie die Rechte und Pflichten der Nutzer klar und deutlich kommunizieren. Da der Skeptiker gewohnt ist, Inhalte im Netz kritisch zu hinterfragen, ist es wichtig, Hintergrundinformationen mit Details über das Angebot und die Rechte und Pflichten der Nutzer zur Verfügung zu stellen. Der Skeptiker nutzt das Internet oft zur Informationsbeschaffung, er liest Zeitungen, informiert sich über soziale Netzwerkseiten wie Twitter oder browst durch Blogs. Da die Qualität von Beiträgen in Blogs oder auf Bürgerjournalismus-Plattformen auch minderwertig oder nicht gesichert sein können, ist es für den Skeptiker wichtig zu wissen, wer der Absender oder der Autor einer Botschaft ist und welche Intention sich hinter einem Beitrag verbirgt. Deshalb ist für den Skeptiker Transparenz und proaktive Kommunikation von zentraler Bedeutung für die Beurteilung der Vertrauenswürdigkeit eines Anbieters, und zwar nicht nur bei Informationsplattformen, sondern bei allen Arten von Online-Angeboten. Bei der Entscheidung, die Transaktion im Netz durchzuführen oder nicht, ist für ihn auch absolute Kostentransparenz zentral, ansonsten hat er das Gefühl, seine Entscheidung aufgrund falscher oder unvollständiger Tatsachen gefällt zu haben, fühlt sich hintergangen und bricht die Transaktion ab. Er erwartet zum Beispiel, dass keine versteckten Gebühren anfallen, sondern der Anbieter direkt den Endpreis kommuniziert oder dass bei einer einmaligen Transkation keine Abonnement-Verpflichtung eingegangen wird. Anbieter von Online-Geschäftsmodellen müssen deshalb darauf achten, die Nutzer bereits am Anfang des Transaktionsprozesses auf mögliche zusätzliche Kosten und Verpflichtungen aufmerksam zu machen.

Mit Visualisierungen arbeiten

Anbieter von Online-Geschäftsmodellen sollten vermehrt mit grafischen Übersichtselementen arbeiten, denn diese erleichtern den Umgang mit einer Seite. Idealerweise hebt die grafische Darstellung den Mehrwert der Applikation hervor, stellt den Transaktionsablauf dar und weist auf die zentralen Rechte und Pflichten des Nutzers hin. Anbieter sollten darauf achten, dass trotz der vielen zentralen Informationen die Darstellung nicht überladen wirkt, denn sonst könnte das Angebot als zu komplex wahrgenommen und nicht genutzt werden. Der Skeptiker probiert gerne Neues aus und er will auf einen Blick erfassen, um was es bei einem Angebot geht. Er muss schnell erkennen, welche Auflagen oder welche Verbindlichkeiten er mit der Transaktion eingeht. Die Abbildung kann auf der Startseite oder auf der „Über uns"-Seite platziert werden. Die in der vorgehenden Handlungsempfehlung besprochene Angebotstransparenz kann durch klares und übersichtliches Design und anhand von Grafiken unterstützt werden und wirkt vertrauensfördernd. Digital Natives lesen keine Bedienungsanleitungen, sondern verlassen sich für ein erstes Ausprobieren höchstens auf eine Übersichtsgrafik. Deshalb ist es besonders wichtig, dass die Applikation intuitiv bedienbar ist und auf bereits erlernte Schemata oder idealtypische Abläufe zurückgreift.

Optionen aufzeigen

Anbieter von Online-Geschäftsmodellen sollten darauf achten, bei der Registrierung Wahlmöglichkeiten zur Verfügung zu stellen, weil für den Skeptiker die Datenhandhabung der Anbieter entscheidend ist. Der Skeptiker schätzt es, wenn ihm bei der Erstanmeldung Wahlmöglichkeiten zur Verfügung stehen, denn er will selbst entscheiden können, ob er sich nur temporär als Besucher beim Anbieter anmeldet oder ob er sich registrieren und ein Kundenkonto einrichten möchte. Dadurch kann er selbstbestimmt handeln, wird in seiner Entscheidungsfreiheit nicht eingeschränkt und fühlt sich vom Anbieter ernst genommen. Durch Wahlmöglichkeiten wird das Risiko eines Transaktionsabbruchs reduziert und zum Vertrauensaufbau beigetragen. Optionen können zusätzlich durch grosszügige Rückgaberechte, durch zeitnahe Kündigunsfristen oder durch eine einfache Löschung des Accounts unterstützt werden.

Pflichtfelder restriktiv einsetzen

Anbieter von Online-Geschäftsmodellen sollten Pflichtfelder bei der Registrierung restriktiv einsetzen, weil der Skeptiker darauf achtet, welche Daten er für einen Dienst zur Verfügung stellen muss. Anbieter müssen sicherstellen, dass nur diejenigen Daten als Pflichtfelder programmiert werden, welche für den Dienst auch effektiv benötigt werden. Bei Pflichtfeldern, welche nicht intuitiv für den Dienst benötigt werden, erwartet der Skeptiker eine Erklärung, um entscheiden zu können, ob diese die Datenpreisgabe rechtfertigt. Unternehmen müssen deshalb plausibel erklären, weshalb diese Daten benötigt werden. Basiert die Angabe der Daten auf Freiwilligkeit, fühlt sich der Skeptiker ungezwungener und selbstbestimmter und es kann sein, dass er in einem freiwilligen Umfeld mehr persönliche Daten zur Verfügung stellt. Wurden aber zu viele Pflichtfelder definiert, bricht der Skeptiker die Transaktion mit grosser Wahrscheinlichkeit ab. Der restriktive Umgang mit Pflichtfeldern zeigt dem Skeptiker ausserdem, dass der Anbieter die Privacy der Nutzer ernst nimmt, was zusätzlich zum Vertrauensaufbau beiträgt.

Kompetenten Kundenservice bieten

Anbieter von Online-Geschäftsmodellen müssen für den Skeptiker keinen 24-Stunden-Kundenservice zur Verfügung stellen, denn Schnelligkeit ist für ihn kein entscheidendes Kriterium zur Beurteilung der Vertrauenswürdigkeit. Notwendig ist aber ein Kundenservice-Team, welches kompetent und ausführlich auf die Anliegen des Skeptikers eingeht. Wichtig ist, dass beim ersten Kontakt mit dem Kundenservice alle Fragen beantwortet werden, denn Rückfragen schätzt er nicht. Für die Vertrauensbildung ist eine detaillierte Antwort einer schnellen Antwort vorzuziehen. Der Skeptiker weiss, dass insbesondere für kleinere Start-ups der Kundenservice ein wesentlicher Kostenfaktor ist und er erwartet keine Rund-um-die-Uhr-Betreuung. Viel wichtiger ist ihm, dass unterschiedliche Möglichkeiten zur Kontaktaufnahme zur Verfügung stehen, denn der Skeptiker meldet sich aus Sicherheits- und Beweisgründen am liebsten schriftlich beim Unternehmen.

5.2.2.2 Handlungsempfehlungen für den Praktiker (Vertrauenstyp 2)

Der Praktiker fühlt sich in seinen Entscheidungen im Internet sicher, ist geübt im Umgang mit dem Netz, ist fortschrittbegeistert und vertraut der Institution Internet sowie dem Anbieter. Er fühlt sich sicher, weil er den Anbieter im Voraus gründlich analysiert und auf alle vier Vertrauensfaktoren achtet. Er nutzt eher konservative Dienste wie Online-Banking oder Online-Shopping, nicht aber soziale Netzwerkseiten, Ausnahme ist der Microblogdienst Twitter. Er ist ein Digital Immigrant mit grosser Lebenserfahrung und hat sich mit vergleichsweise wenigen Ressourcen viel erarbeitet. Er ist kritisch, fordernd, pingelig, qualitäts- und preisbewusst und vergleicht sehr gerne. Der Praktiker vertraut Menschen generell nicht schnell und hat immer eine latente Angst vor Verletzungen. Er ist wenig gebildet, ist dafür aber der Machertyp und nutzt das Internet als Werkzeug zur Selbstverwirklichung und als Fenster zur Welt. Er honoriert faire Anbieter mit Loyalität, indem er wieder kommt und kanaltreu ist.

Anbieter von Online-Geschäftsmodellen, welche sich für den Praktiker als Nutzer interessieren, sollten folgende Handlungsempfehlungen zum Vertrauensaufbau und zur Pflege von Vertrauen (Abbildung 93) in Betracht ziehen:

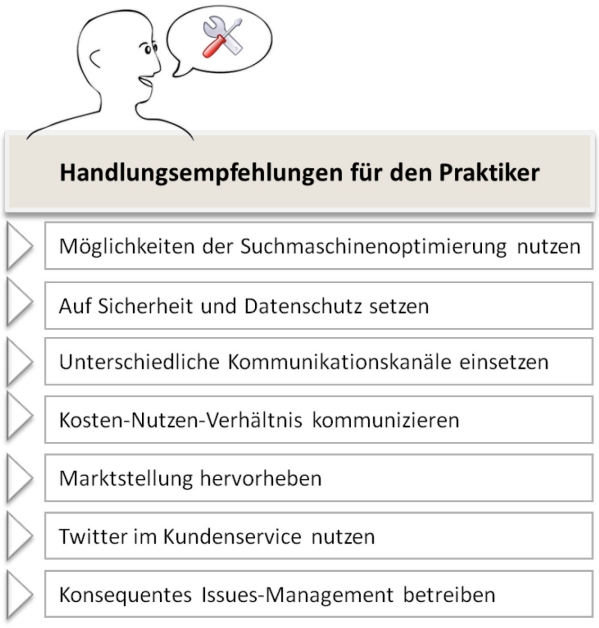


Abbildung 93: Handlungsempfehlungen für den Praktiker (eigene Darstellung)

Möglichkeiten der Suchmaschinenoptimierung nutzen

Um den Praktiker zu erreichen, müssen Anbieter von Online-Geschäftsmodellen die Möglichkeiten der Suchmaschinenoptimierung nutzen. Ziel sollte eine optimale Vernetzung der Seite sein, um bei Suchmaschinen möglichst prominent und weit oben gelistet zu werden. Dazu ist eine permanente Optimierung der Parameter gemäss den von den Suchdiensten definierten Algorithmen nötig. Der Praktiker nutzt unterschiedliche Suchmaschinen, um das Internet nach Informationen zu durchsuchen. Dabei achtet er besonders auf die Listung der Anbieter in den Ergebnissen der jeweiligen Suchmaschinen, denn dies dient ihm als Indiz für eine weite Verbreitung des Portals. Die Auswertungen haben gezeigt, dass der Praktiker auf Alter, Grösse und Bekanntheit eines Anbieters achtet. Er weiss, dass eine Seite mit steigender Beliebtheit und steigendem Verlinkungsgrad weiter oben in der Resultatliste einer Suchmaschine auftaucht. Hohe Suchmaschinenrankings und somit eine hohe Trefferliste seiner Suchanfrage weisen für ihn auf die Wichtigkeit und die Relevanz einer Seite hin und generieren Vertrauen. Die Einhaltung der ethischen Richtlinien ist für den Praktiker elementar, das heisst, es dürfen keine Brückenseiten oder Linkfarms programmiert werden. Ausserdem sollten Anbieter das virale Word-of-Mouth ihrer Nutzer unterstützen, indem die entsprechende Infrastruktur zur Verfügung gestellt wird (zum Beispiel eine Community, ein Blog oder ein Wiki) oder Weiterempfehlungen aktiv belohnt werden. Wichtig ist aber, dass auf keinen Fall Kundenrezensionen selbst geschrieben oder manipuliert werden.

Auf Sicherheit und Datenschutz setzen

Anbieter von Online-Geschäftsmodellen müssen Sicherheitsaspekte und Datenschutz proaktiv ansprechen und thematisieren, weil Datenschutz ein zentrales Anliegen des Praktikers ist. Der Praktiker will wissen, welche Daten für wie lange und für welchen Zweck gespeichert werden; deshalb sollte das Unternehmen den Praktiker über die Handhabung seiner persönlichen Daten stets aufklären. Obwohl der Praktiker hohes Vertrauen in die Institution Internet wie auch in den Anbieter selbst hat, sind Sicherheit und Datenschutz für ihn von enormer Wichtigkeit. Er handelt im Netz sehr wohlüberlegt und es fällt auf, dass der Praktiker eher konservative Seiten mit hohen Sicherheitsstandards nutzt. Der Praktiker geht davon aus, dass die Verfügungsgewalt über die Daten beim Nutzer liegt und bei der Registrierung nicht auf den Anbieter übergeht. Deshalb sollten Anbieter transparent aufzeigen, welche Da-

ten für Werbezwecke verwendet oder an Drittparteien weitergeleitet werden. Der Praktiker reagiert sensibel auf die Weitergabe seiner Daten an Dritte, weshalb darauf ausdrücklich verzichtet werden sollte. Ausserdem sollten Anbieter auf Passwortschutz, Sicherheitsfragen und Verschlüsselung achten. Eine Möglichkeit, auf einen guten Sicherheitsstandard hinzuweisen, ist es, an Sicherheitstests teilzunehmen und die Zertifikate der unabhängigen Drittparteien prominent auf der Startseite zu platzieren. Ausführliche Testberichte und Rapporte können auf einer Unterseite „Sicherheit und Datenschutz" aufgeführt werden. Um ein konsistentes Bild zu vermitteln, ist es wichtig, dass das Gesagte auch in die Tat umgesetzt wird und dass nur die wirklich relevanten Daten der Nutzer erhoben werden. Das heisst, Anbieter von Online-Geschäftsmodellen, welche Sicherheitsaspekte und Datenschutz in den Vordergrund stellen, müssen sich genau überlegen, welche Felder sie als Pflichtfeld markieren, um für den Praktiker glaubwürdig zu sein.

Unterschiedliche Kommunikationskanäle einsetzen

Anbieter von Online-Geschäftsmodellen sollten unterschiedliche Kommunikationskanäle nutzen, online wie offline, damit der Praktiker als Digital Immigrant optimal angesprochen werden kann. Der Praktiker liest täglich seine Zeitung in gedruckter Ausgabe und hört zum Morgenkaffee seinen Lieblings-Radiosender. Deshalb ist es wichtig, dass Unternehmen ihre Bemühungen zur Vertrauensbildung nicht nur auf den Online-Bereich konzentrieren, sondern dass vertrauensbildende Massnahmen über unterschiedliche Kanäle kommuniziert werden. Denkbar sind Kampagnen in Print-Medien, über Plakate, im Radio oder im Fernsehen. Ist der Praktiker interessiert, mehr über das Produkt oder die Dienstleistung zu erfahren, macht er schnell den Schritt von der Offline- in die Online-Welt. Hat der Praktiker bereits einmal von einem Online-Anbieter gehört, ist der Wiedererkennungseffekt gross und die Aufmerksamkeit ist gesichert. Dabei ist wichtig, dass der Anbieter Hintergrundinformationen zum Unternehmen und zum Angebot zur Verfügung stellt. Der Praktiker will wissen, wer hinter einem Angebot steht und wie das Portal entstanden ist. Ausserdem sollte der Anbieter seine Nutzer auch ausserhalb der eigenen Seite betreuen (z. B. in Fachforen oder Chats) und dort Informationen anbieten, wo der Praktiker auch tatsächlich danach sucht (z. B. auf YouTube).

Kosten-Nutzen-Verhältnis kommunizieren

Es ist elementar, dass der Anbieter das Kosten-Nutzen-Verhältnis klar aufzeigt und dass auf mögliche zusätzliche Verpflichtungen proaktiv eingegangen wird, da der Faktor Reziprozität für den Praktiker von besonderer Bedeutung für die Einschätzung der Vertrauenswürdigkeit eines Anbieters ist. Der Praktiker will ohne grossen Aufwand sehen, was ihn die Nutzung des Angebots kostet, und die Kosten müssen als Totalbetrag ersichtlich sein. Fallen während des Transaktionsprozesses zusätzliche, vorher nicht erwähnte Gebühren oder Kosten an, bricht der Praktiker die Transaktion umgehend ab. Der Praktiker hat besondere Freude am Vergleichen und recherchiert deswegen gerne und oft im Netz. Trotzdem ist er kein Schnäppchenjäger, die Qualität des Angebotes und das Vertrauen in den Anbieter stehen im Vordergrund, auch wenn der Preis (oder die geforderten persönlichen Daten) in einem für ihn passenden Verhältnis zum Angebot stehen muss. Ausserdem will der Praktiker vor Abschluss einer Transaktion ausführlich über seine Rechte und Pflichten informiert sein, das heisst, er muss in der Lage sein, die AGBs schnell ausfindig zu machen und diese auch zu verstehen. Anbieter müssen demnach auf verständliche Formulierungen und eine übersichtliche Darstellung achten. Der Praktiker sucht insbesondere nach Informationen zu Garantien, Rückgaberechten oder den Lieferkonditionen, deshalb sollten Qualität und Leistungen garantiert werden. Bei den AGBs ist eine Reduzierung auf das Wesentliche vorzuziehen.

Marktstellung hervorheben

Anbieter von Online-Geschäftsmodellen sollten in ihrer Online- und Offline-Kommunikationsarbeit hervorheben, dass sie ein bekanntes Portal sind, da der Praktiker stark auf die Marktmacht eines Anbieters im Netz achtet. Dies kann durch Hinweise über das Alter des Unternehmens, über die Anzahl der Nutzer oder über die Portalgrösse kommuniziert werden. Unterstützend wirken ausserdem Nutzerempfehlungen, Rankings und Drittparteienzertifizierungen. Marktmacht und Bekanntheit sind für den Praktiker ein Indiz dafür, dass es sich um einen seriösen, vertrauenswürdigen, qualitativ hochstehenden Anbieter handeln muss. Dabei achtet er insbesondere auf stimmiges Design, den Markenauftritt und auf die Listung bei Suchmaschinen. Ausserdem muss auf ein authentisches Erscheinungsbild geachtet werden, welches sich über den gesamten Auftritt des Unternehmens erstreckt. Der Markenauftritt sollte durch ein prägnantes Alleinstellungsmerkmal einen hohen

Wiedererkennungseffekt aufweisen, sodass der Praktiker beim Browsen und Surfen das Design und die Marke des Unternehmens schnell identifizieren kann.

Twitter im Kundenservice nutzen

Online-Anbieter sollten darauf achten, dass der Kundenservice über unterschiedliche Kanäle erreichbar ist. Der Praktiker erwartet vom Kundenservice, dass er schnell, einfach und freundlich ist und dass er unterschiedliche Möglichkeiten zur Kontaktaufnahme zur Verfügung stellt. Der Praktiker kann die Qualität des angebotenen Kundenservice sehr schnell bewerten und besteht darauf, dass seine Anliegen ernst genommen werden. Der Praktiker schätzt zwar konventionelle Customer-Hotlines, reagiert aber bei endlosen Warteschlaufen genervt und tendiert dazu, das Telefonat abzubrechen. Deshalb ist es wichtig, dass bei jeder Kontaktmöglichkeit auch genügend geschultes und freundliches Personal einsatzbereit ist. Die Auswertungen haben gezeigt, dass sich der Praktiker beim Microblogdienst Twitter engagiert, er twittert selbst und steht in regelmässigem Kontakt mit seinen Followern. Auch Anbieter von Online-Geschäftsmodellen sollten den Kommunikationskanal Twitter für ihren Kundenservice in Betracht ziehen, um so mit dem Praktiker zu kommunizieren und ihn mit Informationen zu versorgen. Der Praktiker schätzt unkomplizierte Kanäle und dialogorientierte Kommunikation auf gleicher Augenhöhe erzeugt bei ihm Vertrauen. Durch Twitter wird es möglich, sich kompetent auf das Anliegen des Praktikers vorzubereiten, bevor mit ihm Kontakt aufgenommen wird und der Praktiker kann in der Zwischenzeit weiter im Internet browsen.

Konsequentes Issues-Management betreiben

Ein konsequentes Issues-Management in den Sozialen Medien ist für Anbieter von Online-Geschäftsmodellen von grosser Bedeutung. Der Praktiker sucht bei offenen Fragen oftmals in Fachforen und Chats nach Antworten und stellt dort auch seine Fragen. Anbieter müssen beobachten, ob seine Fragen richtig beantwortet werden und allenfalls – im Namen des Unternehmens – detailliertere Auskünfte erteilen. Wichtig ist für den Praktiker, dass seine Fragen beantwortet werden, wer diese beantwortet, ist für ihn jedoch sekundär. Anbieter müssen deshalb dort reagieren und den Praktiker betreuen, wo er über seine Unklarheiten redet. Für den Praktiker wirkt es kompetent und vertrauensfördernd, wenn sich der Anbieter auch ausserhalb des eigenen Portals um seine Nutzer kümmert, dazu ist aber ein konsequentes Issues-

Management nötig. Der Praktiker ist ein geübter Internetgänger und er weiss, was er von Anbietern zu erwarten hat. Stimmt die versprochene mit der erhaltenen Leistung nicht überein, beschwert er sich zuerst beim Kundendienst. Reagiert dieser jedoch nicht umgehend und in angemessener Form, zögert der Praktiker nicht lange und macht seinem Ärger Luft: Er schreibt negative Rezensionen, bewertet den Anbieter schlecht oder schreibt über sein Erlebtes in einem Blog. Um Diskussionen rund um das Unternehmen und die Marke im Internet nicht zu verpassen, ist es für Anbieter von Online-Geschäftsmodellen besonders wichtig, ein konsequentes Issues-Management zu betreiben. Kritische Stimmen im Internet müssen ernst genommen werden und es muss ein Bewusstsein dafür entstehen, dass jederzeit irgendwo im Netz eine Diskussion entstehen kann, welche im schlimmsten Fall zu einem Shitstorm[55] heranwächst. Das Netz muss deshalb durch Monitoring regelmässig überwacht und ausgewertet werden, damit auf Kritik angemessen und zeitnah reagiert werden kann. Die Reaktion auf Kritik sollte wohlwollend sein und mit der Absicht geschrieben werden, den Fehler in Zukunft zu vermeiden. Die erste Reaktion des Anbieters muss schnell, dialogorientiert, direkt, in angemessener Tonalität und an dem Ort einsetzen, wo die Kritik geäussert wurde.

5.2.2.3 Handlungsempfehlungen für den Sozialen (Vertrauenstyp 3)

Der Soziale hat starkes Vertrauen in die Menschen, ist generell vertrauensvoll und Kontakte in der realen Welt sind für ihn zentral. Beziehungen zu realen Menschen sind ihm wichtig und er vertraut auch seinem ausgewählten Anbieter, weil er weiss, dass hinter jedem Anbieter auch Menschen stehen. Das Internet ist für ihn nur Mittel zum Zweck, in das für ihn abstrakte System Internet an sich hat er wenig Vertrauen. Der Soziale ist kein intensiver Internetnutzer, er ist definitiv kein Vorreiter im Netz, sondern ein eher passiver Online-Kunde. Der Soziale befindet sich bei den Auswertungen und im Typenvergleich auffällig oft im Mittelfeld. Er achtet während einer Transaktion im Internet auf die Marke und das Design, den Kundenservice sowie auf das Reziprozitätsverhältnis. Weniger wichtig ist ihm, wer die Kontrolle über seine persönlichen Daten besitzt, es scheint auch, dass er kein offenes Ohr für Daten-

[55] Ein Shitstorm ist gemäss Duden (2012) ein öffentlicher Sturm der Entrüstung in einem Kommunikationsmedium des Internets, der zum Teil mit beleidigenden Äusserungen einhergeht und dadurch eine sinnvolle Diskussion verhindert.

schutzskandale oder Systempannen hat. Er braucht relativ lange, bis er Vertrauen fasst und den Schritt ins Netz wagt, ist die Transaktion dann aber erfolgreich verlaufen, wird er mit hoher Wahrscheinlichkeit ein Stammkunde werden.

Anbieter von Online-Geschäftsmodellen, welche den Sozialen als Nutzer gewinnen wollen, sollten sich in Bezug auf das Vertrauensmanagement insbesondere auf folgende Handlungsempfehlungen (Abbildung 94) stützen:

Abbildung 94: Handlungsempfehlungen für den Sozialen (eigene Darstellung)

Das Angebot ins Gespräch bringen

Es ist von zentraler Bedeutung, dass Anbieter von Online-Geschäftsmodellen mit ihrem Angebot möglichst viel Aufmerksamkeit generieren, damit dem Sozialen das Portal überhaupt erst auffällt. Ist ein Anbieter in aller Munde, interessiert sich auch der Soziale für das Portal. Damit das Angebot auch in der realen Welt im Gespräch ist, müssen Anbieter von Online-Geschäftsmodellen enorm viele Ressourcen in Werbung und Public Relations investieren. Das heisst, das Angebot sollte im Fernsehen, in den Printmedien oder auf Plakaten zu sehen sein. Möglich ist aber auch eine regionale Präsenz mit lokaler Verwurzelung. Dabei könnte das Unternehmen Vereine oder örtliche Festivitäten unterstützen, um bei der Zielgruppe im Gespräch zu sein. Falls sich das Unternehmen in Ökologie oder Nachhaltigkeit engagiert, sollte dies prominent kommuniziert werden. Denkbar wäre auch eine einmalige Spenden-

Aktion „Helfen im Internet“, bei der 1 Euro pro Transaktion an eine gemeinnützige Organisation gespendet wird. Damit sich der Soziale bei einem Anbieter registriert, muss der Geschäftsmodell-Anbieter mehr bieten als nur das Angebot selbst. Der Soziale ist kein Internet-Enthusiast, sondern er nutzt das Internet und deren Anbieter, um in seiner Community mitreden zu können und mit dabei zu sein. Er möchte sich mit Menschen austauschen und das Internet bietet ihm entsprechende Anknüpfungspunkte und Gesprächsstoff.

In Markenaufbau und -pflege investieren

Anbieter sollten sich auf Markenaufbau und die -pflege konzentrieren und eine starke und bekannte Marke etablieren. Der Soziale ist im Umgang mit dem Internet mässig geübt und achtet deshalb auf Indikatoren von aussen, um die Vertrauenswürdigkeit eines Anbieters einzuschätzen, weshalb eine starke und bekannte Marke für ihn ein wichtiger Hinweis zur Beurteilung eines Anbieters ist. Unternehmen müssen plausibel kommunizieren, dass sie ein bekannter und vertrauenswürdiger Anbieter sind, welcher bereits eine Weile auf dem Markt existiert. Dies kann über Rankings (z. B. Interbrand), über einen Hinweis auf die eigene Marktmacht oder einen Vermerk zur Anzahl der getätigten Bestellungen kommuniziert werden. Auch die Kommuniaktion des Gründungsjahres und somit des Alters wirkt auf den Sozialen vertrauensbildend und kompetent. Durch ein konsequentes Markenmanagement werden Assoziationen beim Sozialen geweckt und das Produkt oder die Dienstleistung wird für ihn differenzierbar und somit auch wiedererkennbar. Ziel der Anbieter sollte eine Emotionalisierung der Marke sein, damit sich der Soziale mit der Marke identifizieren kann.

Erfahrungen von Nutzern einbeziehen

Anbieter von Online-Geschäftsmodellen sollten die Nutzer in den Vordergrund stellen. Online-Anbieter müssen beim Sozialen Überzeugungsarbeit leisten, damit er die Applikation überhaupt erst besucht, und weil für den Sozialen Beziehungen von zentraler Bedeutung sind, sind für ihn Erfahrungen von Nutzern am glaubwürdigsten. Deshalb müssen Anbieter Meinungsführer unter ihren Nutzern ausfindig machen und diese für sich gewinnen. Anbieter von Online-Geschäftsmodellen können zum Beispiel Erfahrungen in Form von Erfolgsgeschichten, Erfahrungsberichten oder kurzen Zitaten von Nutzern auf der Startseite veröf-

fentlichen. Denkbar ist auch der Einsatz von berühmten Personen oder Experten, sogenannten Testimonials, welche öffentlich für das Portal einstehen. Solche Referenzen von realen Menschen zeigen dem Sozialen, dass das Portal genutzt wird und dass man auch zur Nutzung des Portals steht. Für den Sozialen ist eine grosse Anzahl Nutzer ein Indiz dafür, dass der Anbieter einen Mehrwert bietet und vertrauenswürdig ist. Zudem erhöht eine grosse Anzahl Nutzer die Möglichkeit, sich im realen Leben über den Anbieter auszutauschen, und befriedigt somit ein wichtiges Bedürfnis des Sozialen. Anbieter von Online-Geschäftsmodellen sollten demnach auf die Anzahl der Nutzer hinweisen und sie ins Zentrum stellen.

Reale Menschen in den Vordergrund stellen

Anbieter von Online-Geschäftsmodellen sollten nicht nur das Unternehmen selbst vorstellen, sondern auch die Menschen, die hinter dem Unternehmen stehen. Das heisst, es könnten die zentralen Personen, zum Beispiel die Geschäftsleitung sowie das Kundenservice-Team, mit Foto und einer kurzen Beschreibung vorgestellt werden. Diese kann aus einem Zitat über das Unternehmen bestehen, darf aber auch eine persönliche Note beinhalten. Denkbar ist auch eine Vorstellung des gesamten Kundenservice-Teams mit der simplen Botschaft: „Wir sind für Sie da und beraten Sie gerne." Durch das Vorstellen der zentralen Personen des Unternehmens wird dem Sozialen vermittelt, wer hinter dem Angebot steht, wodurch sich für ihn die Hürde verringert, sich zu registrieren. Unterstützend wirken auch Bilder der Geschäftslokalitäten oder eine prominente Platzierung der realen Firmenadresse. Denn Online-Portale sind für den Sozialen nach wie vor etwas Abstraktes und deshalb sollten Anbieter von Online-Geschäftsmodellen nicht nur die Nutzer des Portals, sondern auch die Menschen, welche hinter dem Online-Portal stehen, in den Vordergrund stellen.

Interaktion und Flexibilität fördern

Die Auswertungen haben gezeigt, dass für den Sozialen bei der Beurteilung der Vertrauenswürdigkeit eines Anbieters der Kundenservice von hoher Wichtigkeit ist. Anbieter von Online-Geschäftsmodellen müssen auf einen persönlichen, zeitnahen und flexiblen Kundenservice achten, denn der Soziale wird mit grosser Wahrscheinlichkeit bei Fragen persönlich mit dem Kundenservice Kontakt aufnehmen. Wichtig ist, dass vor, während und nach dem Kauf Unterstützung angeboten wird. Dabei muss der Anbieter von Online-Geschäftsmodellen genügend Personal bereitstellen,

um Anfragen tatsächlich gerecht werden zu können. Um einen zeitnahen Kundenservice zu gewährleisten, könnten auch Avatare als Verstärkung des Kundenservice-Teams eingesetzt werden. Denkbar ist auch das Aufschalten eines Customer-to-Customer-Forums oder einer Diskussionsplattform, auf welcher sich Nutzer untereinander weiterhelfen können. Der Soziale schätzt die Interaktion mit dem Unternehmen oder mit anderen Nutzern; wichtig ist aber schlussendlich, dass seine Fragen kompetent und zeitnah beantwortet werden. Anbieter von Online-Geschäftsmodellen sollten den Kunden entscheiden lassen, über welchen Kanal er mit dem Unternehmen in Kontakt treten möchte, und daher unterschiedliche Möglichkeiten zur Verfügung stellen. Unternehmen sollten ausserdem darauf achten, dass unterschiedliche Zahlungsmethoden angeboten werden, zum Beispiel Bezahlung per Kreditkarte, über PayPal, per Vorkasse und auf Rechnung. Dies signalisiert dem Sozialen die Flexibilität des Anbieters und erzeugt Vertrauen.

Den Nutzer durch den Prozess begleiten

Kundenservice bedeutet für den Sozialen aber auch proaktive Unterstützung während des Transaktionsprozesses. Anbieter von Online-Geschäftsmodellen sollten den Sozialen durch den Transaktionsprozess führen und begleiten. Es wird empfohlen, dem Nutzer nach der Registrierung eine E-Mail zuzustellen, in der er aufgefordert wird, die Registrierung zu bestätigen, oder ihm unmittelbar nach der Bestellung eine Auftragsbestätigung zukommen zu lassen. Er muss über den weiteren Transaktionsablauf informiert werden, zum Beispiel, dass die Bestellung zum Versand bereitsteht oder dass das Paket zum Versand aufgegeben wurde. Der Soziale ist kein intensiver Internetnutzer und deshalb ist es besonders wichtig, dass er sich bei einem Anbieter nicht allein gelassen fühlt. Er darf nicht das Gefühl haben, in einen luftleeren Raum zu bestellen oder sich zu registrieren, ansonsten bricht er die Transaktion ab. Vertrauenswürdig wirkt ausserdem, wenn er jederzeit den Status seiner Bestellung selbst prüfen und nachverfolgen kann. Dadurch fühlt sich der Soziale sicher und aufgehoben und dies wirkt vertrauensstiftend.

Storytelling nutzen

Der Soziale achtet während einer Transaktion stark auf den Faktor Marke und Design. Wichtig ist, dass Anbieter von Online-Geschäftsmodellen ihrem Unternehmen und ihrer Marke ein Gesicht geben, um dem Sozialen ein Gefühl für die Unterneh-

mung zu vermitteln. Dazu eignet sich zum Beispiel das Erzählen der Gründergeschichte. Das Erzählen von Geschichten ist eine der ältesten Methoden zur Kommunikation und auch Anbieter von Online-Geschäftsmodellen sollten sich dieser Methode bedienen. Durch Storytelling können Emotionen geweckt und Vertrauen erzeugt werden, es können Komplexität reduziert und Werte vermittelt werden und das virtuelle Unternehmen wird durch Storys realer und anschaulicher. Mit lebendigen und spannenden Geschichten gewinnt man Aufmerksamkeit und kann das Unternehmen auf sympathische Art vorstellen. Denn die gesellschaftliche Komponente eines Unternehmens ist für den Sozialen von enormer Bedeutung. Ausserdem speichert der Soziale Geschichten besser, erzählt sie weiter und betreibt so Mund-zu-Mund-Propaganda für das Unternehmen. Die Geschichten sollten kurz und prägnant formuliert sein und können mit Fotos oder Videos unterlegt werden.

Im folgenden Kapitel werden die Stärken und Limitationen der vorliegenden Dissertation besprochen.

5.3 Stärken und Limitationen der vorliegenden Arbeit

Wie jeder Forschungsprozess ist auch die vorliegende Arbeit auf einen im Voraus definierten Themenbereich beschränkt. Ziel dieser Arbeit war es, die Bedeutung von Vertrauen bei Transaktionen in Online-Geschäftsmodellen aufzuzeigen und einen Beitrag zum tieferen Verständnis von Vertrauen im Internet zu leisten. Die vorliegende Dissertation differenziert die Wahrnehmung von Vertrauen anhand von Vertrauenstypen und behandelt dadurch ein in der Literatur sehr wenig beachtetes Teilgebiet der Vertrauensforschung. Die in dieser Arbeit ermittelten Vertrauensfaktoren zeigten eine sehr hohe Validität bei der Zuverlässigkeit der Messung der Ergebnisse (Cronbachs Alphas lagen deutlich über dem Grenzwert). Dies kann darauf zurückzuführen sein, dass die in der Theorie generierten Vertrauensfaktoren durch die qualitativen Interviews überprüft und verdichtet wurden, bevor sie in der qualitativen Umfrage anhand einzelner Items abgefragt wurden. Es scheint, dass eine solche Herangehensweise ein richtiger Weg ist, das komplexe Forschungsfeld Vertrauen anzugehen. Eine weitere Stärke dieser Arbeit ist sicherlich auch die hohe Fallzahl der Online-Umfrage mit 1'549 ausgefüllten Fragebögen. Dadurch wurde es möglich, die einzelnen Cluster im Detail auszuwerten, miteinander zu vergleichen und aussagekräftige Analysen zu treffen.

Die vorliegende Arbeit unterliegt jedoch einigen Einschränkungen und Limitationen, welche nicht unerwähnt bleiben dürfen. Diese Arbeit hat sich auf einen kleinen Teilbereich der Vertrauensforschung konzentriert. Einzelne Aspekte mussten für diese spezifische Analyse bewusst aussen vor gelassen werden. Es wäre zum Beispiel interessant, neben Vertrauen auch das Misstrauen der Nutzer zu untersuchen. Dies könnte weitere Hinweise auf das Verhalten der Nutzer und einen vertieften Einblick bei der Entscheidungsfindung im Internet generieren. Darüber hinaus hat sich diese Arbeit auf Vertrauensfaktoren fokussiert, welche vom Unternehmen direkt beeinflussbar sind. Es existieren in der Literatur weitere Einflussfaktoren, wie zum Beispiel der Staat, der Rechtsrahmen oder die Medien, welche in dieser Studie keine Beachtung fanden. Für ein vollumfängliches Verständnis von Vertrauen müssten weitere Einflussfakten in die Analyse miteinbezogen werden.

Für diese Forschungsarbeit wurden Internetnutzer, welche in Deutschland wohnen, und Online-Anbieter, welche auf dem deutschen Markt tätig sind, befragt. Diese Konzentration auf Deutschland macht es schwierig, die Studienergebnisse zu generalisieren. Zum Beispiel ist Privacy – und somit auch Privacybedenken – ein westliches

Konstrukt, welches auf dem Individuum aufbaut, welches zum Beispiel in asiatischen Ländern anders aussehen würde (Burk, 2007; Zureik & Harling Stalker, 2010). Internationale Unternehmen, welche im Online-Bereich tätig sind, haben jedoch Nutzer aus der ganzen Welt. Diese Studie hat leider nicht untersucht, inwiefern die in dieser Arbeit diskutierten Resultate auf einen internationalen Nutzerstamm übertragbar sind. Interessant wäre es, Unterschiede in Bezug auf das Land, die Kultur oder die Sprachregion zu identifizieren und Online-Anbietern aufgrund dessen weitere Handlungsempfehlungen vorschlagen zu können. Die Autorin ist der Meinung, dass insbesondere die Kommunikation und die visuelle Gestaltung von Botschaften über das Internet sehr kulturabhängig und somit unterschiedlich sind.

Eine weitere Limitation dieser Arbeit ist, dass die Befragung der Probanden online stattgefunden hat. Somit besteht die Möglichkeit, dass sich durch diese Arbeit ein digitaler Graben (Digital Divide) zieht. Durch die Integration der telefonisch und persönlich geführten qualitativen Interviews in der Voruntersuchung wurden dennoch Aspekte netzfernerer Zielgruppen in die Analyse miteinbezogen und der digitale Graben konnte wenigstens teilweise überbrückt werden.

Diese Arbeit hat drei unterschiedliche Vertrauenstypen identifiziert und charakterisiert. In der realen Geschäftswelt kann es jedoch problematisch sein, das Nutzerportfolio in eine fixe Anzahl von Gruppen einzuteilen. Es kann sein, dass die Datenbasis für eine Einteilung nicht vorhanden ist, der Nutzerstamm sehr divers ist und eine Gruppierung keinen Sinn ergibt oder aber dass sich das Nutzerportfolio sehr schnell verändert. Die Identifikation von Vertrauenstypen ist bei langfristigen Beziehungen zwischen Unternehmen und Nutzer durchaus sinnvoll, nicht aber bei hohen Nutzerfluktuationsraten. Deshalb denkt die Autorin, dass die Handlungsempfehlungen von den Anbietern von Online-Geschäftsmodellen nur bedingt direkt aus dieser Forschungsarbeit übernommen werden können. Daher ist es wichtig, dass die Aussagen nicht als absolut angesehen, sondern eher als richtungsweisend verstanden werden.

Diese Arbeit hat nicht spezifisch nach Online-Geschäftsmodellen differenziert. Zwar wurde die Nutzung als Kriterium bei der Unterscheidung miteinbezogen, interessant wäre es jedoch, die Vertrauenstypen und die Einflussfaktoren pro Online-Geschäftsmodell zu identifizieren und diese dann zu vergleichen. Die Autorin ist der Meinung, dass nicht nur hinsichtlich des Vertrauenstyps grosse Unterschiede bestehen, sondern ebenfalls hinsichtlich der einzelnen Geschäftsmodelle. Auch das Kommunikationsverhalten und die Kultur unter den Nutzern innerhalb eines Geschäfts-

modells variieren stark und dies kann ebenfalls Auswirkungen auf die Vertrauensbildung haben. Diese erweiterten Analysen hätten jedoch den Umfang dieser Arbeit gesprengt und wären mit der erhobenen Fallzahl auch nicht sinnvoll gewesen.

In dieser Arbeit wurde der Fokus auf die relativen Mittelwerte der einzelnen Faktoren gelegt. Zusätzlich wäre es interessant, noch die absoluten Mittelwerte zu besprechen. Ziel der Arbeit ist es jedoch, die Unterschiede der Vertrauenstypen hervorzuheben und zu diskutieren, und dafür ist der relative Mittelwert massgeblich. Würden pro Faktor jeweils zwei unterschiedliche Mittelwerte angegeben, würden die Ergebnisse unübersichtlich und unklar. Deshalb wurde auf die Angabe des absoluten Mittelwertes als Zusatzinformation verzichtet.

Jedes Forschungsvorhaben ist eingebettet in einen spezifischen technischen, zeitlichen und kulturellen Kontext. Die Erfahrungen mit und Erwartungen an technische Systeme verändern sich durch Innovationen und neue gesellschaftliche Wahrnehmungen von Chancen und Risiken rasant und stellen Nutzer wie auch Anbieter vor immer neue Herausforderungen. Es kann sein, dass sich die Wahrnehmung der Nutzer bei der Fertigstellung dieser Arbeit bereits wieder verschoben hat.

5.4 Ausblick

Das folgende Kapitel 5.4.1 stellt konkrete Anknüpfungspunkte für weitere Forschungsaktivitäten vor und Kapitel 5.4.2 wagt einen Blick in die Zukunft der Vertrauensforschung.

5.4.1 Bereiche mit weiterem Forschungspotenzial

Dieses Kapitel zeigt aus Sicht der Autorin interessante weitere Bereiche auf, bei welchen noch Forschungspotenziale und Forschungslücken bestehen.

Mitarbeiter und Unternehmenskultur: Aus der Perspektive des Unternehmens wie auch der Wissenschaft wäre es interessant herauszufinden, inwiefern der Mitarbeiter bei der Bildung von Nutzervertrauen direkt oder indirekt einen Einfluss hat. Der Autorin ist aufgefallen, dass der Mitarbeiter als Schnittstelle zum Unternehmen in der Vertrauensliteratur sehr wenig Beachtung findet. Weiter wäre es interessant zu erforschen, ob unterschiedliche Unternehmenskulturen einen Einfluss auf das Nutzervertrauen haben. Die Unternehmenskultur beeinflusst die Umgangsformen und somit die Kommunikationskultur eines Unternehmens nach innen und aussen. Inwiefern wird dies von den Nutzer wahrgenommen und über welche Faktoren?

Globale Geschäftsbeziehungen: Dass Unterschiede hinsichtlich des Vertrauens zwischen den Kulturen bestehen, konnte durch verschiedene Studien nachgewiesen werden (Shankar et al., 2002; Gefen, 2000; Lee & Turban, 2001). Jedoch wurden keine Studien gefunden, die Aussagen darüber machen, wie sich diese Unterschiede konkret äussern. Das Vertrauen ist von Natur aus eigentlich eine sehr lokale Angelegenheit, heutige globale Geschäftsbeziehungen und das Internet heben das Vertrauen der Nutzer jedoch auf eine neue Stufe. Inwiefern sind bestehende Forschungsergebnisse auf andere Kulturen übertragbar? Was sind die regionalen Unterschiede, was die internationalen Gemeinsamkeiten bei der Wahrnehmung von Vertrauen? Worauf können sich international tätige Unternehmen verlassen? Gibt es global gültige Vertrauensfaktoren, welche angewendet werden können? Welche Stolpersteine in Bezug auf Vertrauen müssen globale Unternehmen kennen?

Nichtnutzer: Diese Arbeit hat unter anderem diskutiert, dass viele Nutzer aufgrund fehlenden Vertrauens in die Institution Internet oder in die Anbieter den Schritt ins Netz nicht wagen. Eine hohe Internetnutzung ist jedoch für eine gesamte

Volkswirtschaft von grossem Interesse. Kann das Vertrauensmanagement von Unternehmen dazu beitragen, dass in Zukunft Nicht-Internetnutzer zu Nutzern werden? Könnte durch Empfehlungen von Drittparteien in der realen Welt das Vertrauen in die Institution Internet gefördert werden? Welchen Einfluss haben Dritte, zum Beispiel der Staat oder die Medien? Welche Stellhebel müssen von wem getätigt werden?

Längsschnittstudien: In dieser Arbeit wurde darauf hingewiesen, dass Vertrauen als Prozess betrachtet werden sollte. Der Grossteil der Studien ist jedoch noch immer statischer Natur (Urban et al., 2009). Zukünftige Forschung könnte in einer Längsschnittstudie das effektive Verhalten der Nutzer messen und nachvollziehen, anstatt nur die hypothetischen Absichten zu evaluieren. Um die zeitliche Entwicklung von Vertrauen abzubilden, könnte die Internetnutzung von einer Probandengruppe zum Beispiel über drei Monate hinweg beobachtet werden. Längsschnittstudien zu Vertrauen wären auch mit Fokus auf die Beziehung zwischen dem Nutzer und dem Anbieter spannend. Weiter interessant zu erforschen wären die einzelnen Phasen von Vertrauen über die Zeit: Wie kann in welcher Phase bei wem Vertrauen erzeugt werden? So könnten Aussagen zur Dynamik von Vertrauen gemacht werden.

Skalenentwicklung: Über verschiedene Disziplinen hinweg wird Vertrauen anders definiert, interpretiert und gemessen. Eine einheitliche Skala zur Messung von Vertrauen würde die vielen Studien vergleichbarer machen und dazu führen, dass Forschungsarbeiten aufeinander aufbauen könnten. Deshalb wäre es ein wichtiger Beitrag an die Forschungsgemeinde, eine in den unterschiedlichen Disziplinen einsetzbare und verankerte Skala zu entwickeln, welche sich als Standard etablieren würde.

Personalisierung und Vertrauen: Im Literaturteil dieser Arbeit wurde diskutiert, dass Online-Anbieter immer mehr personalisierte Dienstleistungen anbieten, auch ohne dass dies dem Nutzer immer bewusst ist. Diese Personalisierung kann zu einem Informationsverlust führen, insbesondere, wenn Resultate von Suchmaschinen individualisiert werden. Neue, unkonventionelle Inputs können zu neuen Ideen und Lösungen führen, welche jedoch durch einen strikten Algorithmus auch abgewürgt werden können. Dieser Umstand wird nach und nach von Nutzern wahrgenommen und von den Medien thematisiert. Diese mediale Aufmerksamkeit wird nach Meinung der Autorin noch zunehmen. Die Frage ist nun, welche Einstellung Internetnutzer gegenüber personalisierten Produkten und Dienstleistungen haben. Steigt das Vertrauen in den Anbieter aufgrund der Personalisierung oder ist das Gegenteil der

Fall? Sinkt das Vertrauen durch die gesteigerten Personalisierungstendenzen der Wirtschaft oder macht sich die Mehrheit der Nutzer diesbezüglich keine Gedanken?

Sanktionsmöglichkeiten: Interessant wäre es zu erforschen, ob Sanktionsmöglichkeiten einen Einfluss auf Transaktionen im Netz haben. Sanktionen könnten Bewertungen, Ratings oder Ausschlussanträge sein. Bestehen für den Nutzer Möglichkeiten, die zu vertrauende Partei bei Nichteinhalten der versprochenen Leistung zu sanktionieren, nimmt er dann eher an der Transaktion teil? Kann das Vertrauen der Nutzer durch Sanktionsmöglichkeiten gesteigert werden? Haben Versicherungen Einfluss auf die Risikowahrnehmung und das Nutzervertrauen?

Interdisziplinäre Forschung: Wie im Theoriekapitel erläutert, interessieren sich ebenso Rechtswissenschaftler wie Wirtschaftswissenschaftler für die Sorgen und Bedenken der Nutzer im Internet. Auch Psychologen und Soziologen befassen sich seit Jahren mit Vertrauen und dem Vertrauensaufbau. Bei der Literaturrecherche ist aufgefallen, dass im Bereich Vertrauensforschung im Internet sehr wenig interdisziplinär geforscht wird. Zwar werden die Forschungsergebnisse gegenseitig reflektiert und integriert, es wird jedoch selten gemeinsam nach neuen Ansätzen gesucht. Spannend wäre es nun, als interdisziplinäres Forschungsteam das Thema Vertrauen im Internet zu ergründen, um dadurch neue Aspekte in die aktuelle Diskussion einbringen zu können.

Unterschiedliche Forschungsmethoden: Der wichtigste Aspekt des Vertrauensmanagements ist der Einfluss auf die Zielgruppe selbst, und deshalb sollte der Einfluss auf die Vertrauensbildung auch immer bei der Zielgruppe untersucht werden. Besonders interessant wäre es, mit Internetnutzern Experimente am Bildschirm durchzuführen. Zum Beispiel könnten die in dieser Arbeit besprochenen Vertrauensfaktoren auf speziell dafür programmierten Seiten unterschiedlich dargestellt und anhand einer Conjoint-Analyse abgefragt werden. Dadurch könnten die Einflussfaktoren auf die Zielgruppe im Detail eruiert werden. Eine weitere Möglichkeit wäre, Tiefeninterviews mit den Nutzern zu führen. Durch die Interviewmethode des Laddering wäre es zum Beispiel möglich, die Beweggründe hinter dem Vertrauen der Nutzer zu eruieren und mehr über die Motive zu erfahren.

Sensibilität und Menge der abgefragten Daten: In der Literatur wurde diskutiert, dass die Nutzer nicht alle persönlichen Daten als gleich sensibel einstufen. Als wenig sensibel zum Beispiel gelten Beruf, Zivilstand oder Altersklasse und als sensibel gelten Kreditkartennummer, Kreditwürdigkeit oder Passwörter. Die Autorin geht da-

von aus, dass persönliche Nutzerprofile in Zukunft enorm an Wert gewinnen werden. In dieses Forschungsfeld wird bereits in naher Zukunft sehr viel mehr Bewegung kommen und viele neue Online-Anbieter werden versuchen, sich in diesem Bereich zu etablieren. Spannend zu erforschen wäre es, ob sich die Bereitschaft, persönliche Daten zur Verfügung zu stellen, verändert, wenn die abgefragten Daten für die Transaktion Sinn ergeben bzw. wenn der Nutzer nicht erkennen kann, weshalb er die geforderten Daten für diesen Service angeben muss (Krankheitsgeschichte bei einem Zeitungsabonnement). Darüber hinaus wäre es interessant zu eruieren, ob Internetnutzer sich die Menge der angegebenen Information über die Zeit merken. Spielt der Zeitpunkt der Datenerhebung für die Menge der abgefragten Daten eine Rolle? Können über gestaffelte Erhebungen mehr oder weniger Daten der Nutzer erhoben werden? Sind die Nutzer bereits so weit sensibilisiert, dass schlanke Nutzerprofile ein Profilierungsmerkmal für Anbieter darstellen? Honorieren Nutzer Unternehmen mit schlanken Nutzerprofilen bzw. sanktionieren sie die Sammelwut von Unternehmen?

Im letzten Kapitel dieser Dissertation wird nun ein Blick in die Zukunft des Forschungsthemas gewagt.

5.4.2 Ein Blick in die Zukunft

Das Zusammenspiel von Vertrauen im Internet und Bedenken bezüglich der Privatheit wird nach Meinung der Autorin in Zukunft immer wichtiger werden und an Brisanz zunehmen. Früher schützte der zeitliche und räumliche Abstand die Privatsphäre der Individuen, in unserer technologiebasierten Wissensgesellschaft brauchen wir dafür neue Normen. Die Privacy der Internetnutzer wird national, aber auch international von einer Vielzahl von Gesetzen, Verordnungen und Richtlinien geschützt. Da je nach Land oder Region unterschiedliche Rechtsauffassungen bestehen, ist eine einheitliche internationale Regelung momentan nicht in Sicht. Die Gesellschaft muss über die Praktiken zur Datenspeicherung der Unternehmen umfassend informiert sein, damit jedes Individuum frei entscheiden kann, wie restriktiv oder freizügig es mit seinen persönlichen Daten im Netz umgehen will, und weiss, welche Konsequenzen diese Entscheidung hat. Jeder Internetnutzer und Konsument muss selbst anfangen, sich und seine privaten Daten im Netz zu managen. Ideal wäre es, wenn sich der Nutzer Kenntnisse über die Marketingpraktiken von Unternehmen aneignen und sich über Strategien zu seinem Schutz informieren würde.

Der Science-Fiction-Schriftsteller Isaac Asimov schreibt zum Thema Privacy der Zukunft: "The advance of civilization is nothing but an exercise in the limiting of privacy." Genau gegenteilig argumentiert die politische Schriftstellerin Ayn Rand: "Civilization is the progress toward a society of privacy." Asimov argumentiert, dass es durch Technologien wie das Internet immer einfacher wird, persönliche Informationen zu sammeln und aufzuarbeiten. Rand wiederum begründet ihre These damit, dass die freie und kompetitive Marktwirtschaft aus Eigeninteresse die individuelle Privacy beschützen werde. Die Wissenschaftler Rust et al. (2009) fragten sich, wer von diesen beiden nun recht habe, und kommen zum Schluss, dass die Zukunft möglicherweise eine Mischung aus der Sichtweise von Asimov und Rand sein wird. Die Autoren stimmen zu, dass Privacy in Zukunft abnehmen wird, nicht aber verschwindet, da gleichzeitig die Industrie zum Schutz der Privacy wächst, der Schutz der Privacy aber immer teurer wird (Rust et al., 2009).

Könnte es sein, dass wir unsere Privacy ein Stück weit aufgeben zugunsten einer transparenten Gesellschaft, in der alles in der Öffentlichkeit stattfindet? Beurteilt man anhand der Überschriften der Boulevard-Presse, könnte man genau dies meinen. Dort wird impliziert, dass Nutzer durch den Gebrauch von sozialen Netzwerken immer mehr Daten der Öffentlichkeit zur Verfügung stellen, ohne über die Kon-

sequenzen nachzudenken. Die Autorin ist jedoch der Meinung, dass momentan und in naher Zukunft ein Paradigmenwechsel in Bezug auf das Verständnis von privaten Daten im Netz stattfindet und weiterhin stattfinden wird.

Erst jetzt werden sich Nutzer langsam, aber sicher über die Konsequenzen der kommerziellen Datensammlung bewusst und die mediale Aufmerksamkeit widmet sich vermehrt diesem Thema. Geübte Internetnutzer wissen jedoch sehr wohl, welche Informationen sie wo veröffentlichen und haben gegenüber den Unternehmen auch klar den Anspruch, diese Daten zu schützen. Unternehmen werden von Seiten der Medien und der Politik, vom Gesetzgeber, von internationalen Organisation, aber auch vom Nutzer selbst gezwungen werden, transparent zu kommunizieren, wie Nutzerdaten gehandhabt werden. Transparenz wird in Zukunft zum Differenzierungsmerkmal und Unternehmen sollten sich heute schon darauf einrichten. Ausserdem wird es eine Kernaufgabe für Unternehmen sein, Kundenprofile und Nutzerdaten sicher vor Dritten zu schützen. Genau hier liegt das Potenzial der Unternehmen, Vertrauen zu generieren und sich auf dem Markt der Zukunft zu positionieren.

Für Unternehmen bedeutet dies, dass in Zukunft mehr in den Vertrauensaufbau investiert werden muss. Vertrauen ist der Ursprung jeder Transaktion, egal welches Medium genutzt wird. Doch je innovativer Geschäftsmodelle sind und je mehr Technik hinter einem Angebot steht, desto unsicherer ist der Nutzer und je höher ist das wahrgenommene Risiko. Beim Cloud-Computing liegen die Daten beispielsweise in unbekannten Rechenzentren an unbekannten Orten auf der Welt. Voraussetzung für die Nutzung dieser Angebote ist Vertrauen ins Medium Internet und in den Anbieter. Für die Zukunft kann dies bedeuten, dass das Vertrauen der Nutzer anhand eines gezielten Monitorings gemessen und gepflegt werden muss und als Aktivposten in Form des Goodwills eines Unternehmens in die Bücher einfliesst. Unternehmen, welche bei ihren Nutzern heute schon Vertrauen erzeugen und erhalten können, werden auch diejenigen sein, welche langfristig Erfolg haben.

In der Einleitung dieser Dissertation wurde darauf hingewiesen, dass unsere Kommunikationsgesellschaft momentan im Begriff ist, sich vom Informationszeitalter zu lösen, um sich ins Datenzeitalter zu klicken (Schuppisser, 2012). Je mehr Daten andere über uns zur Verfügung haben und je besser diese Daten aufbereitet werden, desto transparenter und entblösster werden wir – aber ebenso unser Gegenüber (Metzler, 2012). Wir müssen also neue Wege finden und es müssen sich neue Normen und Werte etablieren, um die totale Durchsichtigkeit von uns zu akzeptieren

und unserem Nächsten zu verzeihen. Der Internetphilosoph David Weinberg schlussfolgert: “An age of transparency must be an age of forgiveness.” (Jarvis, 2009, S. 232).

6 Literatur- und Quellenverzeichnis

(N)Onliner Atlas. (2012). *(N)Onliner Atlas 2011. Deutschlands grösste Studie zur Internetnutzung. Initiative D21.* Gefunden am 15. März 2012 unter www.initiatived21.de/portfolio/nonliner-atlas

100days. (2012). *Starseite 100 Days*. Gefunden am 11. März 2012 unter www.100-days .net/

Aaker, D. (1995). Building strong brands. *Brandweek, 36* (37), 28–34.

Aaker, D. (2000). *Brand leadership*. New York: Free Press.

Acquisti, A. & Gross, R. (2007). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Lecture notes in computer science, 4258*, 36–58.

Afuah, A. & Tucci, C. L. (2001). *Internet Business Models and Strategies*. Boston: McGraw-Hill.

Alby, T. & Karzauninkat, S. (2007). *Suchmaschinenoptimierung: professionelles Website-Marketing für besseres Ranking.* (2. Auflage). München: Hanser.

Amelung, U. (2002). *Der Schutz der Privatheit im Zivilrecht*. Tübingen: Mohr.

Anderson, Ch. (2007). *The Long Tail*. Nischenprodukte statt Massenmarkt – Das Geschäft der Zukunft. München: Carl Hanser Verlag.

Anderson, R. E. & Srinivasan, S. (2003). E-Satisfaction and E-Loyalty: A Contingency Framework. *Psychology and Marketing* 20 (2), 123–138.

Andrade, E. B., Kaltcheva V. D. & Weitz, B. A. (2002). Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Company Reputation. *Advances in Consumer Research 29 (*1), 350–353.

Andressen, T. (2010). *Erfolgreiches Strategisches Management des E-Procurement*. In: R. Bogaschewsky, M. Essig, R. Lasch & W. Stölzle. (Hrsg.). Supply Management Research. Wiesbaden: Gabler.

Antil, J. H. (1984). Conceptualization and Operationalization of Involvement. *Advances in Consumer Research*, *11* (1), 203–209.

APA. (2012). *Interbrand Ranking*. Gefunden am 11. März 2012 unter www.medianet.at/fileadmin/main/pictures/Okt2011/061011/interbrand_ranking400.jpg

Applegate, L. (2000). *E-Business Models: Making Sense of the Internet Business Lanndscape*. In G. Dickson and G. DeSanctis. (Hrsg.).Information Technology and the Future Enterprise, New Models for Managers. Upper Saddle River NJ: Prentice Hall, 49–101.

Argenti, P. A. (1998). *Corporate Communication*. Boston: McGraw-Hill.

Arminger, G. (1979). *Faktorenanalyse. Statistik für Soziologen*. Stuttgart: Teubner.

Arrington, M. (2010). *Interview mit Mark Zuckerberg vom 11. Januar 2010*. TechCrunch. Gefunden am 06. Dezember 2010 unter www.amitechnology.vodspot.tv/video/2839774-facebooks-zuckerberg-says-the-age-of-privacy-is-over

Ashworth, L. & Free, C. (2006). Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns. *Journal of Business Ethics*, 67 (2), 107–123.

Assael, H. (1998). Consumer Behavior and Marketing Action. (6. Auflage). Cincinnati, Ohio: South Western College.

Augsburger Allgemeine. (2009, 31. Oktober). Datenklau bei SchülerVZ: Verdächtiger nimmt sich das Leben. Augsburger Allgemeine. Gefunden am 05. Januar 2010 unter www.augsburger-allgemeine.de/Home/Nachrichten/Aus-aller-Welt/Artikel,-datenklau-schueler-VZ-Selbstmord-_arid,1963138_regid,2_puid,2_pageid,4293.html

Bacher, J., Pöge, A. & Wenzig, K. (2010). *Clusteranalyse. Anwendungsorientierte Einführung in Klassifikationsverfahren*. (3. Auflage). München: Oldenbourg.

Backhaus, K., Erichson, B., Plinke, W. & Weiber, R. (2011). *Multivariate Analysemethoden. Eine anwendungsorientierte Einführung.* (13. Auflage). Berlin: Springer.

Bähring, K., Hauff, S., Sossdorf, M. & Thommes, K. (2008). Methodologische Grundlagen und Besonderheiten der qualitativen Befragung von Experten in Unternehmen: Ein Leitfaden. *Swiss Journal of Business Research and Practice, 1*, 89–110.

Bailey, K. D. (1994). *Typologies and Taxonomies: An Introduction to Classification Techniques*. Los Angeles: Sage Publications Inc.

Balocco, R., Rangone, A., Cardano, P. & Valacca, R. (2004). The role of E-Malls in B2C e-commerce: a classification framework and the comparison between Italian and US cases. *International Journal of Electronic Business*, 2 (2), 1.

Bambury, P. (1998). *A Taxonomy of Internet Commerce.* First Monday 3 (10). Gefunden am 30. Dezember 2012 unter www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/624/545

Barnes, S. (2006). A Privacy Paradox: Social Networking in the United States. *First Monday, 11 (9)*. Gefunden am 25. August 2009 unter www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394

Barrera, M. H. & Okai, J. M. (1999). Digital Correspondence: Recreating Privacy Paradigms. *International Journal of Communications Law and Policy*, 3. Gefunden am 28. Mai 2011 unter www.austlii.edu.au/au/journals/MurUEJL/1999/14.html

Barrigar, J., Burkell, J. & Kerr, I. (2006). Let's not get psyched out of privacy: reflections on withdrawing consent to the collection, use and disclosure of personal information. *Canadian Business Law Journal*, 44 (1), 54–71.

Bart, Y., Shankar, V., Sultan, F. & Urban, G. (2005). Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study. *Journal of Marketing*, 69 (4), 133–152.

Batinic, B. (2001). Datenqualität bei internetbasierten Befragungen. In: A. Theobald, M. Dreyer & T. Starsetzki (Hrsg.). *Online Marktforschung: Theoretische Grundlagen und praktische Erfahrungen*. Wiesbaden: Gabler, 119–132.

Bauhofer, B. (2004). *Reputation Management. Glaubwürdigkeit im Wettbewerb des 21. Jahrhunderts*. Zürich: Orell Füssli.

Bawden, D. & Robinson, L. (2009). The dark side of information: overload, anxiety and other paradoxes and pathologies. *Journal of Information Science*, 35 (2), 180–191.

Bawden, D. (2001). Information and digital literacies: a review of concepts. *Journal of Documentation*, 57 (2), 218–259.

Beaudoin, C. E. (2008). Explaining the relationship between Internet use and interpersonal trust: Taking into account motivation and information overload. *Journal Of Computer-Mediated Communication*, 13 (3), 550–568.

Belanger, F. & Crossler, R. E. (2011). Privacy In The Digital Age: A Review Of Information Privacy Research In Information Systems. *MIS Quarterly*, 35 (4), 1017–1041.

Belanger, F. & Hiller, J. S. (2006). A framework for e-government: privacy implications. *Business Process Management Journal*, 12 (1), 48–60.

Belanger, F., Hiller, J. S. & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, 11 (3–4), 245–270.

Benn, S. I. (1971). *Privacy, Freedom, and Respect for Persons*. In: R. J. Pennock & J. W. Chapman (Hrsg.). Privacy. New York: Atherton Press, 1–26.

Bergs, S. (1981). *Optimalität bei Cluster-Analysen. Experimente zur Bewertung numerischer Klassifikationsverfahren*. Münster: Universität Münster.

Berry, L. (2000). Cultivating Service Brand Equity. *Journal of the Academy of Marketing Science, 28* (1), 128–137.

Betz, F. (2002). Strategic Business Models. *Engineering Management Journal 14 (1)*: 21–27.

Bhatnagar, A., Misra, S. & Rao, H. R. (2000). On risk, convenience and internet shopping behavior. *Communications of the ACM, 43* (11), 98–105.

Bhattacherjee, A. (2002). Individual Trust in Online Firms: Scale Development and Initial Test. *Journal of Management Information Systems, 19* (1), 211–241.

Blacksocks. (2012). *Kennen Sie das Original Socken-Abo? bei Blacksocks*. Gefunden am 11. März 2012 unter www.blacksocks.com/g3.cms/lang/de/s_page/77750/s_name/abo

Blackwell, R. D., Miniard, P. W. & Engel, J. F. (2001). Consumer Behavior. (9. Auflage). Fort Worth: Harcourt College Publishers.

Blattberg, R. C. & Deighton, J. (1991). Interactive marketing: Exploiting the age of addressability. *Sloan Management Review, 1*, 5–14.

Blau, P. M. (1964). *Exchange and power in social life*. New York: Wiley.

Bloustein, E. (1964). Privacy as an Aspect of Human Dignity. *New York University Law Review,* 39 (6), 962–1007.

Bourdieu, P. (1983). *Ökonomisches Kapital, kulturelles Kapital, soziales Kapital.* In: R. Kreckel (Hrsg.). Soziale Ungleichheiten. (Soziale Welt Sonderband 2), Göttingen: Schwartz, 183–198.

Bowie, N. E. & Jamal, K. (2006). Privacy Rights on the Internet: Self-Regulation or Government Regulation? *Business Ethics Quarterly,* 16 (3), 323–342.

Boyd, D. (2007). Why Youth (Heart) Social Network Sites: The Role of Networked Publics. In: D. Buckingham (Hrsg.). *Youth, Identity and Digital Media*. Cambridge, MA: MIT Press, 119–142.

Brace, I. (2004*). Questionnaire Design: How to plan, structure and write survey material for effective market research*. London: Kogan Page.

Brandeis, L. (1914). Other Peoples Money and How the Bank Use It. In: R. H. Weber. Transparency and the governance of the Internet. *Computer Law & Security Review*, 24 (4), 2008, 342–348.

Brashers, D. E., Adkins, M. & Meyers, R. A. (1994). Argumentation and computer-mediated group decision making. In: L. R. Frey (Hrsg.). *Group communication in context: Studies of natural groups*. Hilsdale, NJ: Erlbaum, 263–282.

Breuer, S. & Brenner, W. (2004). Geschäftsmodelle internetbasierter Unternehmen. In: K. Stanoevska-Slabeva (Hrsg.). *The Digital Economy – Anspruch und Wirklichkeit*. Berlin: Springer.

Brinkmann, U. & Seifert, M. (2001). „Face to interface“: Zum Problem der Vertrauenskonstitution im Internet am Beispiel von elektronischen Auktionen. *Zeitschrift für Soziologie, 30* (1), 23–47.

Brosius, F. (2008). *SPPS 16 für Dummies. Statistische Analyse statt Datenchaos*. (2. Auflage). Weinheim: Wiley.

Bucher, E., Fieseler, Ch. & von Kaenel, A. (2009). Web 2.0 – Eine Annäherung an die Herausforderungen des neuen Internetzeitalters aus Sicht der Unternehmenskommunikation. In: G. Bentele, M. Piwinger & G. Schönborn (Hrsg.). *Kommunikationsmanagement. Strategien, Wissen, Lösungen*. Neuwied: Luchterhand, 1–24.

Buchmann, E., Bohm, K. & Raabe, O. (2008). Privacy2.0: Towards Collaborative Data-Privacy Protection. In: Proceedings of the IFIPTM'08, 2008. Gefunden am 10. Januar 2012 unter www.ipd.kit.edu/~buchmann/pdfs/buchmann08privacy20.pdf

Burk, D. L. (2007). *Privacy and property in the global datasphere*. In: S. Hongladarom & C. Ess (Hrsg.). Technology Ethics: Cultural Perspectives, Hershey, PA: Idea Group Reference , 94–107.

Cai, X. & Gantz, W. (2000). Online privacy issues associated with web sites for children. *Journal of Broadcasting & Electronic Media, 44* (2), 197–214.

Casalo, L. V., Flavian, C. & Guinaliu, M. (2008). Fundaments of trust management in the development of virtual communities. *Management Research News, 31* (5), 324–338.

Cespedes, F. V. & Smith, H. J. (1993). Database Marketing: New Rules for Policy and Practice. *Sloan Management Review, 34*, 7–22.

Chadwick, S. A. (2001). Communicating trust in e-commerce interactions. Management *Communication Quarterly, 14* (4), 653–658.

Chau, P. Y. K., Au G. & Tam K. Y. (2000). Impact of Information Presentation Modes on Online Shopping: An Empirical Evaluation of a Broadband Interactive Shopping Service. *Journal of Organizational Computing & Electronic Commerce, 10* (1), 1–21.

Chellappa, R. & Sin, R. (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management, 6* (2–3), 181–202.

Chellappa, R. K. & Shivendu, S. (2010). Mechanism Design for "Free" but "No Free Disposal" Services: The Economics of Personalization Under Privacy Concerns. *Management Science, 56* (10), 1766–1780.

Chen, K. & Rea, A. I. (2004). Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques. *Journal of Computer Information Systems, 44* (4), 85–92.

Chen, Y. H. & Barnes, S. (2007). Initial Trust and Online Buyer Behavior. *Industrial Management and Data Systems*, 107 (1), 21–36.

Cheskin/Sapient. (1999*). eCommerce trust study*. Cheskin Research and Studio Archetype. San Francisco: Business Wire.

Cho, J. (2006). The mechanism of trust and distrust formation and their relational outcomes. *Journal of Retailing*, 82 (1), 25–35.

Christofides, E., Muise, A. & Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *CyberPsychology & Behavior, 12* (3), 341–345.

Cineman. (2012). *Mein Cockpit bei Cineman*. Gefunden am 11. März 2012 unter www.cineman.ch/memberzone/profil/data.php

Clemmer, E. C. & Schneider, B. (1996). Fair Service. In: T. A. Swartz, D. E. Bowen & S. W. Brown, *Advances in Services Marketing and Managemen.* Greenwich, CT: JAI Press, 109–126.

Coleman, J. S. (1988). Social capital in creation of human capital. *American Journal of Sociology*, 94, 95–120.

Cook, D. & Luo, W. (2003). The Role of Third-Party Seals in Building Trust Online. *e-Service Journal, 2* (3), 71–84.

Cook, J. & Wall, T. (1980). New work attitude measures of trust, organizational commitment and personal need non-fulfillment. *Journal of Occupational Psychology*, 53, 39–52.

Corbitt, B., Thanasankit, T. & Yi, H. (2003). Trust and e-commerce: a study of consumer perceptions. *Electronic Commerce Research & Applications, 2* (3), 203–215.

Corritore, C. L., Kracher, B. & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. International Journal Of Human-Computer Studies, 58 (6), 737–758.

Coulter, K. & Coulter, R. (2002). Determinants of trust in a service provider: the moderating role of length of relationship. *Journal of Services Marketing*, 16 (1), 35–50.

Cranor, L., Reagle, J. & Ackerman, M. (2000). Beyond Concern: Understanding Net Users' Attitudes about Online Privacy. In: I. Vogelsang & B. M. Compaine (Hrsg.). *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy*. Cambridge, MA: The MIT Press, 47–70.

Crawford, S. D., Couper, M. P. & Lamias, M. J. (2001). Web-surveys: Perceptions of burdens. *Social Science Computer Review, 19* (2), 146–162.

Culnan, M. J. & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science, 10* (1), 104–115.

Culnan, M. J. & Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues, 59* (2), 323–342.

Culnan, M. J. (1995). Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing. *Journal of Direct Marketing, 9*, 10–19.

Culnan, M.J. (2000). Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy & Marketing, 19* (1), 20–26.

Currall, S. C. & Judge, T. A. (1995). Measuring Trust Between Organizational Boundary Role Persons. *Organizational Behavior and Human Decision Processes*, 64, 151–170.

Darley, W. K., Blankson, C. & Luethge, D. J. (2010). Toward an integrated framework for online consumer behavior and decision making process: A review. *Psychology & Marketing*, 27 (2), 94–116.

Das, T. K. & Teng, B.-S. (1998). Between trust and control: Developing confidence in partner cooperation in alliances. *Academy of Management Review, 23* (3), 491–512.

Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13* (3), 319–340.

Davis, F., Bagozzi, R. & Warshaw, P. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, *35* (8), 982–1003.

DaWanda. (2012). *Reisetasche Leder auf DaWanda*. Gefunden am 11. März 2012 unter www.dawanda.com/product/27706593-Reisetasche-Leder

Deichsel, G. & Trampisch, H. J. (1985). *Clusteranalyse und Diskriminanzanalyse*. Stuttgart: Gustav Fischer.

DeinDeal. (2012). *Freunde einladen bei DeinDeal*. Gefunden am 11. März 2012 unter www.deindeal.ch/refer-friends

Denzin, N. K. (1983). Interpretative Interactionism. In: G. Morgan (Hrsg.), *Beyond Method: Strategies for Social Research*. London: Sage.

Destatis (2010a). Statistisches Bundesamt Deutschland. Bevölkerung nach Altersgruppen, Familienstand und Religionszugehörigkeit. Gefunden am 07. Dezember 2010 unter www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Statistiken/Bevoelkerung/Bevoelkerungsstand/Tabellen/Content75/AltersgruppenFamilienstand,templateId=renderPrint.psml

Destatis (2010b). Statistisches Bundesamt Deutschland. Bevölkerungsstand. Gefunden am 07 Dezember 2010 unter www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Navigation/Statistiken/Bevoelkerung/Bevoelkerungsstand/Bevoelkerungsstand.psml;jsessionid=12CEA236A6EA7451E2658057FCBFC841.internet2

Deutsch, M. (1958). Trust and suspicion. *Journal of Conflict Resolution, 2*, 265–279.

Dimitriadis, S. & Kyrezis, N. (2010). Linking trust to use intention for technology-enabled bank channels: The role of trusting intentions. *Psychology & Marketing*, 27 (8), 799–820.

Dinev, T. & Hart, P. (2005). Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal Of Electronic Commerce*, 10 (2), 7–29.

Dinev, T. & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17 (1), 61–80.

Dommeyer, C. J. & Gross, B. L. (2003). What Consumers Know and What They Do: An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies. *Journal of Interactive Marketing, 17* (2), 34–51.

Doney, P. & Cannon, J. (1997). An examination of the nature of trust in the buyer-seller relationship. *Journal of Marketing*, 61 (2), 35–51.

Doodle. (2012). *Startseite Doodle*. Gefunden am 11. März 2012 unter www.doodle.com/

Dressler, M. & Telle, G. (2009). *Meinungsführer in der interdisziplinären Forschung: Bestandsaufnahme und kritische Würdigung*. Wiesbaden: Gabler.

DRS 2. (2012, 20. Februar). *Crowdfunding: Mäzenatentum für die kleine Brieftasche*. Gefunden am 21. Februar 2012 unter www.drs.ch/www/de/drs/themen/digital/323959.crowdfunding-maezenatentum-fuer-die-kleine-brieftasche.html

Drüeke, R. & Weber, K. (2007). *Mobile Internetdienste und Privatsphäre. Theoretische Überlegungen und empirische Daten zu einem vieldeutigen Konzept.* Arbeitsberichte Internet Business, Nr. 10 (12). Gefunden am 28. Mai 2011 unter www.kuwi.europa-uni.de/de/lehrstuhl/vs/philosophie/forschung/publikationen/Theorien_Privatsphaere.pdf

Dubosson-Torbay, M., Osterwalder, A. & Pigneur, Y. (2002). E-Business Model Design, Classification, and Measurements. *Thunderbird International Business Review, 44* (1), 5–23.

Duden. (2013). Bedeutung Institution. Gefunden am 30. April 2013 unter http://www.duden.de/rechtschreibung/Institution#Bedeutung2

Duden. (2012). Bedeutung Shitstorm. Gefunden am 09. November 2012 unter www.duden.de/rechtschreibung/Shitstorm

Dunfee, T. W., Smith, N. C: & Ross, W. T. (1999). Social Contracts and Marketing Ethics. *Journal of Marketing, 63*, 14–32.

Dürscheid, Ch. (2007). *Private, nicht-öffentliche und öffentliche Kommunikation im Internet*. Neue Beiträge zur Germanistik. Bd. 6 (4), Japanische Gesellschaft für Germanistik, 22–41.

Dyer, J. H. & Chu, W. (2003). The role of trustworthiness in reducing transaction costs and improving performance: Empirical evidence from the United States, Japan, and Korea. *Organization Science*, 14 (1), 57–68.

Dziuban, C. & Shirkey, E. (1974). When is a Correlation Matrix Apropriate for Factor Analysis? *Psychological Bulletin*, 81 (6), 358–361.

Eastlick, M. A., Lotz, S. L. & Warrington, P. (2006). Understanding Online B-to-C Relationships: An integrated Model of Privacy Concerns, Trust and Commitment. *Journal of Business Research, 59* (8), 877–886.

Eat. (2012). *Startseite Eat*. Gefunden am 11. März 2012 unter www.eat.ch/

eBay. (2012). *Startseite eBay*. Gefunden am 11. März 2012 unter www.ebay.de/

Eckey, H.-F., Kosfeld, R. & Rengers, M. (2002). *Multivariate Statistik. Grundlagen – Methoden – Beispiele.* (1. Auflage). Wiesbaden: Gabler.

eDarling. (2012). *Startseite eDarling*. Gefunden am 11. März 2012 unter www.edarling.de/

Edwards, L. & Brown, I. (2009). Data Control and Social Networking: Irreconcilable Ideas? In: A. Matwyshyn. (Hrsg.). *Harboring Data: Information Security, Law and the Corporation*. Stanford, CA: Stanford University Press, 202–227.

Egger, F. (2000). "Trust me, I'm an online vendor": towards a model of trust for e-commerce system design. *Proceedings of the CHI '00 extended abstracts on Human factors in computing systems*. New York: ACM Press., 101–102.

Egger, F. N. (2001). Affective Design of E-Commerce User Interfaces: How to Maximise Perceived Trustworthiness. In: M. Helander, H. M. Khalid & M. P. Tham (Hrsg.). *Proceedings of CAHD2001: Conference on Affective Human Factors Design*. Singapore, 317–324.

Einwiller, S., Herrmann, A. & Ingenhoff, D. (2005). *Vertrauen durch Reputation – Grundmodell und empirische Befunde im E-Business.* Marketing – Zeitschrift für Forschung und Praxis (Marketing ZFP), 1, 25–42.

Eisenmann, T. (2002). *Internet business models, text and cases*. New York, McGraw-Hill Irwin.

Ellison, N., Steinfield, C. & Lampe, C. (2007). The benefits of Facebook "friends:" social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12* (4), 1143–1168.

Engel, J. F., Blackwell, R. D. & Miniard, P. W. (1986). Consumer Behaviour. (5. Auflage). Hinsdale: Dryden Press.

Engel, J. F., Kollat, D. T. & Blackwell, R. D. (1968). Consumer Behaviour. New York: Holt, Rinehart & Winston.

Engel, J. F., Kollat, D. T. & Blackwell, R. D. (1978). Consumer Behaviour. (3. Auflage). Hinsdale: Dryden Press.

Enzweiler, T. (2008). Ohne Vertrauen geht nichts. Gefunden am 21. März 2012 unter www.welt.de/debatte/kommentare/article6073645/Ohne-Vertrauen-geht-nichts.html

Ergenzinger, R. & Thommen, J.-P. (2005). Marketing. Vom klassischen Marketing zu Customer Relationship Management und E-Business. Zürich: Versus.

Essoussi, L. H. & Zahaf, M. (2009). Exploring the decision-making process of Canadian organic food consumers. *Qualitative Market Research: An International Journal*, 12 (4), 443–459.

Euijin, K. & Tadisina, S. (2007). A Model of Customers Trust in e-Businesses: Micro-Level Inter-Party Trust Formation. *Journal Of Computer Information Systems*, 48 (1), 88–104.

Fan, W. & Tsai, M. (2010). Factors driving website success – the key role of Internet customisation and the influence of website design quality and Internet marketing strategy. *Total Quality Management & Business Excellence, 21* (11), 1141–1159.

Fang, X. & Salvendy, G. (2003). Customer-Centred Rules for Design of e-Commerce Web Sites. *Communications of the ACM, 46* (12), 332–336.

Fassnacht, M. & Köse, I. (2007). Consequences of Web-based service quality: Uncovering a multi-faceted chain of effects. *Journal of Interactive Marketing, 21* (3), 35–54.

Fieseler, Ch. & Meckel, M. (2009). Die Moral der Unternehmenskommunikation: Lohnt es sich, gut zu sein?. In: Siegfried J. Schmidt, Jörg Tropp (Hrsg.): *Die Moral der Unternehmenskommunikation*. Köln: Herbert von Halem Verlag, 124–138.

Fischer, C., Keil-Slawik, R. & Richter, A. (2001). *Verhaltensprofile im Internet*. R. Keil-Slawik (Hrsg.). Digitale Medien und gesellschaftliche Entwicklung. Arbeit, Recht und Gemeinschaft in der Informationsgesellschaft. Berlin: Waxmann.

Fleck, M., Meckel, M. & von Kaenel, A. (2010). Web 2.0 Concepts, Social Software and Business Models. In: I. Lee (Hrsg.). *Encyclopedia of E-Business Development and Management in the Global Economy*. Hershey, Pennsylvania: IGI Global., 1183–1192.

Flesch, R. (1949). *The Art of Readable Writing*. New York: Macmillan.

Flick, U. (2002). *Qualitative Sozialforschung. Eine Einführung*. Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag GmbH.

Focus. (2009, 10. Februar). Schlitzaugen-Gag. Cyrus entschuldigt sich. Gefunden am 14. Dezember 2012 unter www.focus.de/panorama/boulevard/schlitzaugen-gag-cyrus-entschuldigt-sich_aid_370008.html

Fombrun, C. J. (1996). *Reputation. Realizing Value from the Corporate Image*. Boston: Harvard Business School Press.

Foxman, E. R. & Kilcoyne, P. (1993). Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues. *Journal of Public Policy & Marketing, 12* (1), 106–119.

Franke, N., Keinz, P. & Steger, C. (2009). Testing the Value of Customization: When Do Customers Really Prefer Products Tailored to Their Preferences?. *Journal of Marketing*, 73 (5), 103–121.

Fraser, M. & Dutta, S. (2009). *Throwing Sheep in the Boardroom – How Online Social Networking Will Transform Your Live, Work and World.* West Sussex: Wiley.

Fried, Ch. (1968). Privacy. *Yale Law Journal, 77* (3), 475–493.

Friedman, B. A., Kahn, P. H. & Howe, D. C. (2000). Trust Online. *Communications of the ACM, 43 (12)*, 34–40.

FTC – Federal Trade Commission. (1998). *Privacy Online. A Report to Congress.* Washington, DC: Federal Trade Commission. Gefunden am 29. November 2010 unter www.ftc.gov/reports/privacy3/priv-23a.pdf.

FTC – Federal Trade Commission. (2000). *Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress.* Washington, DC: Federal Trade Commission. Gefunden am 29. November 2010 unter www.ftc.gov/reports/privacy2000/ privacy2000.pdf.

Fukuyama, F. (1995). Trust: The Social Virtues and the Creation of Prosperity. New York: The Free Press.

Fukuyama, F. (1996). Trust still Counts in a Virtual World. *Forbes, 158* (13), 33–69. Gefunden am 26. Januar 2010 unter www.search.ebscohost.com/login.aspx?direct=true&db=buh&AN=9611198070&loginpage=login.asp&site=ehost-live

Galegher, J. Sproull, L. & Kiesler, S. (1998). Legitimacy, authority and communication in electronic support group. *Written Communication,* 15, 493–530.

Gandy, O. (1993). *The Panoptic Sort: A Political Economy of Personal Information*. New York: Westview.

Ganesan, S. (1994). Determinants of long-term orientation in buyer-seller relationship. *Journal of Marketing*, 58 (2), 1–19.

Garfinkel, S. (2000). Privacy and the new technology. *Nation*, 270 (8), 11–15.

Gasser, U. (2011, 15. Mai). Aufmerksamkeit ist im Internet die neue Währung. *NZZ am Sonntag*, 36–37.

Gasser, U., Cortesi, S. & Palfrey, J. (2011). *The Changing Role of the Individual for Privacy: The Example of Youth Online.* OECD Buch. Manuskript zur Veröffentlichung unterbreitet.

Gates, G. (2010). *Facebook Privacy: A Bewildering Tangle of Options* (12. Mai 2010). Gefunden am 12. April 2012 unter www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html

Gavison, R. (1980). Privacy and the Limits of Law. *Yale Law Journal, 89* (3), 421–471.

Gefen, D. & Straub, D. W. (2003). Managing User Trust in B2C e-Services. *e-Service Journal, 2* (2), 7–24.

Gefen, D. (2000). E-Commerce: The role of familiarity and trust. Omega: The International *Journal of Management Science, 28* (6), 725–737.

Gefen, D. W. (2003). Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly*, 27 (1), 51–90.

Geider, F. J., Rogge, K.-E. & Schaaf, H. P. (1982). *Einstieg in die Faktorenanalyse*. Heidelberg: Quelle & Meyer.

Getty, J. P. (ohne Datum). Zitate – Jean Paul Getty. Gefunden am 21. April 2012 unter www.zitate.net/jean%20paul%20getty.html

Geyskens, I., Steenkamp, J.-B. E. M. & Kumar, N. (1998). Generalizations about trust in marketing channel relationships using meta-analysis. *International Journal of Research in Marketing, 15 (3)*, 223–248.

Giffen, M. (2008). Online Privacy. *Current Health,* 34 (7), 8–11.

Glaser, B. G. & Strauss, A. (1967). *The discovery of Grounded theory: strategies for qualitative research.* New York: Aldine De Gruyter.

Gläser, J. & Laudel, G. (2006). *Experteninterviews und qualitative Inhaltsanalyse*. Wiesbaden: VS Verlag.

Glazer, R. (2001). Marketing in an information-intensive environment: Strategic implications of knowledge as an asset. *Journal of Marketing, 55*(4), 1–19.

Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Garden City, NY: Doubleday.

Goodwin, C. (1991). Privacy: Recognition of a Consumer Right. *Journal of Public Policy & Marketing, 10* (1), 149–166.

Google. (2012). *Informationen über das Unternehmen Google*. Gefunden am 11. März 2012 unter www.google.ch/intl/de/about/corporate/company/

Gouldner, A. W. (1960). The norm of reciprocity. *American Sociological Review*, 25, 547–562.

Grabner-Kräuter, S. & Kaluscha, E. A. (2003). Empirical research in on-line trust: A Review and critical assessment. *International Journal Of Human-Computer Studies*, 58 (6), 783–812.

Graham, J. P. (1987). Privacy, Computers, and the Commercial Dimensions of Personal Information. *Texas Law Review, 65* (7), 1395–1439.

Grant, I. C. (2006). Online Privacy: An Issue for Adolescents. *Proceedings of the Child and Teen Consumption Conference*. Copenhagen.

Greif, B. (2009, 22. Oktober). SchülerVZ-Datendiebstahl: 20-Jähriger wegen versuchter Erpressung verhaftet. *ZDNet.de*. Gefunden am 05. Januar 2010 unter www.zdnet.de/news/wirtschaft_sicherheit_security_schuelervz_datendiebstahl_20_jaehriger_wegen_versuchter_erpressung_verhaftet_story-39001024-41516081-1.htm

Griffin, K. (1967). The contribution of studies of source credibility to a theory of interpersonal trust in the communication process. *Psychological Bulletin*, 68, 104–120.

Guay, D. & Ettwein, J. (1998). Internet commerce basics. *Electronic Markets*, 8 (1), 12–15.

Güntner, J. (2010, 14. April). Digitaler Exhibitionismus. *Neue Zürcher Zeitung*. Gefunden am 29. April 2012 unter www.nzz.ch/nachrichten/kultur/aktuell/digitaler_exhibitionismus_1.5440117.html

Ha, H-Y. & Perks, H. (2005). Effects of consumer perceptions of brand experience on the web: Brand familiarity, satisfaction and brand trust. *Journal of Consumer Behaviour, 4* (6), 438–452.

Haes, J. (2003). Netzwerkeffekte im Medien- und Kommunikationsmanagement: Vom Nutzen sozialer Netze. Wiesbaden: Gabler.

Hagel, I. I. I. J. & Armstrong, A. (1997). *Net Gain: Expanding Markets Through Virtual Communities.* Boston: Harvard Business School Press.

Hank, R. (2008). Vertrauen in die Märkte. Spring doch einfach! Frankfurter Allgemeine (09. Februar 2008). Gefunden am 24. April 2012 unter www.faz.net/aktuell/wirtschaft/wirtschaftsbuecher/vertrauen-in-die-maerkte-spring-doch-einfach-1516283.html

Hargittai, E. (2002). Second-Level Digital Divide: Differences in People's Online Skills. *First Monday*, 7 (4), 1–19.

Harper, Ch. (1998). *And That's the Way It Will Be: News and Information in a Digital World*. New York: New York University Press.

Harris, C. (1997). Developing online market research methods and tools – considering theorizing interactivity: models and cases. *Marketing & Research Today, 25* (4), 267.

Harris, L. & Goode, M. (2004). The four levels of loyalty and the pivotal role of trust: a study of online service dynamics. *Journal of Retailing, 80* (2), 139–158.

Hart, C. & Blackshaw, P. (2005). Communication breakdown. *Marketing Management, 14* (6), 24–30.

Hart, P. & Saunders, C. (1997). Power and Trust: Critical Factors in the Adoption and Use of Electric Data Interchange. *Organization Science, 8* (1), 23–42.

HAW-Hamburg. (2012). *Studienwahl Navigator der HAW-Hamburg*. Gefunden am 11. März 2012 unter www.haw-hamburg.de/nc/news-single/article/schon-100000-registrierte-nutzer-beim-studienwahl-navigator.html

Heath, R. L. & Bryant, J. (2000). *Human communication theory and research*. Hillsdale, NJ: Erlbaum.

Heidemann, B. (10. Oktober 2008). Schwerpunt Vertrauen: Es tut gut, sich auf andere verlassen zu können. Gefunden am 20. August 2012 unter www.derwesten.de/waz-info/es-tut-gut-sich-auf-andere-verlassen-zu-koennen-id1090981.html

Hermes, V. & Thür, H. (2011). *Es tut sich was!* Marketing 2011 / 21. Jahrgang. R. Köhler (Hrsg.). St.Gallen: KünzlerBachmann Medien.

Hewson, C., Yule, P., Laurent, D. & Vogel, C. (2003). *Internet Research Methods*. London: Sage.

Hirsig, R. (2001*). Statistische Methoden in den Sozialwissenschaften: Eine Einführung im Hinblick auf computergestützte Datenanalysen mit SPSS für Windows.* Band 2 (3.Auflage). Zürich: Seismo.

Hoegg, R., Meckel, M., Stanoevska-Slabeva, K. & Martignoni, R. (2006). Overview of business models for Web 2.0 communities. *Proceedings of GeNeMe 2006*. Dresden, 23–37.

Hoffman, D. L. & Novak, T. P. (2009). Flow Online: Lessons Learned and future prospects. *Journal of Interactive Marketing, 23* (1), 23–24.

Hoffman, D. L., Novak, T. P. & Peralta, M. A. (1999a). Building Consumer Trust Online. *Communications of the ACM, 42* (4), 80–85.

Hoffman, D. L., Novak, T. P. & Peralta, M. A. (1999b). Information Privacy in the Marketspace: Implications for the Commercial Use of Anonymity on the Web. *The Information Society, 15* (2), 129–139.

Hoffmann, C. P. & von Kaenel, A. (2009). Sicherheit versus Privatheit im Internet. Vertrauen – aber wie? *Datareport, 4*, 22–24.

Hoffmann, C. P. & von Kaenel, A. (2010a). Online Trust Management: Eine Herausforderung für die Unternehmenskommunikation. In: G. Bentele, M. Piwinger & G. Schönborn (Hrsg.). *Kommunikationsmanagement. Strategien, Wissen, Lösungen*. Neuwied: Luchterhand, 1–26.

Hoffmann, C. P. & von Kaenel, A. (2010b). Vertrauen: Notwendige Grundlage von Online-Transaktionen. In: R. Schliesky (Hrsg.). *Technikgestütztes Identitätsmanagement. Schriften zur Modernisierung von Staat und Verwaltung*. Band 7. Kiel: Lorenz-von-Stein-Institut für Verwaltungswissenschaften.

Hoffmann, C. P., Meckel, M. & von Kaenel, A. (2010a). *Online Vertrauensmanagement: Herausforderung für die Organisationskommunikation.* Beitrag präsentiert an der Jahrestagung der Schweizerischen Gesellschaft für Kommunikations- und Medienwissenschaft (SGKM), 11. Mai 2010, Luzern.

Hoffmann, C. P., Meckel, M. & von Kaenel, A. (2010b). *The Role of Public Relations in Online Trust Management*. 60th Annual Conference of the International Communication Association, 23. Juni 2010, Singapur.

Homans, G. C. (1958). Social Behavior as Exchange. *American Journal of Sociology,* 63, 597–606.

Homburg, Ch. & Giering, A. (1996). Konzeptualisierung und Operationalisierung komplexer Konstrukte – Ein Leitfaden für die Marketingforschung. *Marketing ZFP*, 18, 5–24.

Hopf, Ch. (1991). Qualitative Interviews in der Sozialforschung. Ein Überblick. In: U. Flick, E. v. Kardorff, H. Keupp, L. v. Rosenstiel & S. Wolff (Hrsg.). *Handbuch qualitative Sozialforschung. Grundlagen, Konzepte, Methoden und Anwendungen*. München: Psychologie Verlags Union, 517.

Hoy, M. G. & Phelps, J. (2003). Consumer Privacy and Security Protection on Church Web Sites: Reasons for Concern. *Journal of Public Policy & Marketing, 22* (1), 58–70.

Hoyer, W. D. (1984). An Examination of Consumer Decision Making for a Common Repeat Purchase Product. *Journal of Consumer Research*, 11 (3), 822–829.

Hu, X., Wu, G., Wu, Y. & Zhang, H. (2010). The effects of Web assurance seals on consumers' initial trust in an online vendor: A functional perspective. *Decision Support Systems*, 48 (2), 407–418.

Huber, M. (2008). *Kommunikation im Web 2.0*. Konstanz: UVK.

Hui, K.-L., Tan, B. C. Y. & Goh, C.-Y. (2006). Online Information Disclosure: Motivators and measurements. *ACM Transactions on Internet Technology*, 6 (4), 415–441.

Hunt, S. D., Sparkman, R. D. & Wilcox, J. B. (1982). The Pretest in Survey Research: Issues and Preliminary Findings. *Journal of Marketing Research, 19* (2), 269–273.

Hutter, T. (2011). *Facebook: Infografik und demographische Daten Deutschland, Österreich und Schweiz per Oktober 2011*. Gefunden am 11. Dezember 2012 unter www.thomashutter.com/index.php/2011/11/facebook-infografik-und-demographische-daten-deutschland-osterreich-und-schweiz-per-oktober-2011/

Ikea. (2012). *Frag Anna bei IKEA*. Gefunden am 11. März 2012 unter www.ikea.com/ch/de/

Im, S., Lee, D. H., Taylor, C. R. & D'Orazio, C. (2008). The influence of consumer self-disclosure on Web sites on advertising response. *Journal of Interactive Advertising*, 9 (1), 87–106.

Jackson, D. D. (1980). Familienregeln: Das eheliche Quid pro Quo. In: P. Wazlawick & J. M. Weakland (Hrsg.). *Interaktion*. Bern: Huber.

Jackson, R. & Wang, P. (1994). *Strategic Database Marketing*. Lincolnwood, IL: NTC Publishing.

Jacobs, R. S., Hyman, M. R. & McQuitty, S. (2001). Exchange-specific self-disclosure, social self-disclosure, and personal selling, *Journal of Marketing Theory and Practice*, 9 (1), 48–62.

Jacoby, J. (1975). Consumer psychology as a social psychological sphere of action. *American Psychologist.* 30 (10), 977–987.

Jarvenpaa, S. L. & Tractinsky, N. (1999). Consumer Trust in an Internet Store: A Cross-Cultural Validation. *Journal of Computer-Mediated Communication, 5* (2). Gefunden am 29. November 2010 unter www.onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.1999.tb00337.x/full

Jarvenpaa, S. L., Tractinsky, N. & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management*, 1, 45–71.

Jarvis, J. (2005, ab Juni). *BuzzMachine*. Gefunden am 26. Februar 2012 unter www.buzzmachine.com.

Jarvis, J. (2009). What would Google do? HarperCollins Publishers: New York.

Jevons, C. & Gabbott, M. (2000). Trust, Brand Equity and Brand Reality in Internet Business Relationships: An Interdisciplinary Approach. *Journal of Marketing Management, 16* (6), 619–634.

Jiang, P., Jones, D. B. & Javie, S. (2008). How third-party certification programs relate to consumer trust in online transactions: An exploratory study. *Psychology & Marketing*, 25 (9), 839–858. Dash, S. & Saji, K. B. (2007). The Role of Consumer Self-Efficacy and Website Social-Presence in Customers' Adoption of B2C Online Shopping: An Empirical Study in the Indian Context. *Journal of International Consumer Marketing*, 20 (2), 33–48.

Johnson, D. (2007). Achieving customer value from electronic channels through identity commitment, calculative commitment, and trust in technology. *Journal of Interactive Marketing, 21* (4), 2–22.

Johnson, M. D. & Auh, S. (1998). Customer Satisfaction, Loyalty, and the Trust Environment. *Advances in Consumer Research*, 5, 15–20.

Joinson, A. N., Woodley, A. & Reips, U. (2007). Personalization, authentication and self-disclosure in self-administered Internet surveys. *Computers in Human Behavior, 23* (1), 275–285.

Jones, G. R. & George, J. M. (1998). The experience and evolution ot trust: Implications for cooperation and teamwork. *Academy of Management Review, 23 (3)*, 531–546.

Jones, M. G. (1991). Privacy: A Significant Marketing Issue for the 1990s. *Journal of Public Policy & Marketing, 10 (1)*, 133–148.

Jones, S., Johnson-Yale, C., Millermaier, S. & Pérez, S. F. (2009). Everyday life, online: U.S. college students' use of the Internet. *First Monday, 14* (10). Gefunden am 13. Oktober 2009 unter www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2649/2301

Jones, S., Wilikens, M., Morris, P. & Masera, M. (2000). Trust Requirements in e-Business. *Communications of the ACM, 43* (12), 81–87.

Jourard, S. M. (1966). Some Psychological Aspects of Privacy. *Law and Contemporary Problems, 31* (2), 307–318.

Jourard, S. M. (1971). *Self-Disclosure: An experimental analysis of the transparent self*. New York: Wiley.

Kaiser, H. & Rice, J. (1974). Little Jiffy, Mark IV. *Educational and Psychological Measurement*, 34, 111–117.

Keen, P. G. W., Balance, C., Chan, S. & Schrump, S. (1999). *Electronic Commerce Relationships*: Trust by Design. Englewood Cliffs, NJ: Prentice-Hall.

Kilian, T., Hass, B. H. & Walsh, G. (2007). Grundlagen des Web 2.0. In: B. H. Hass, G. Walsh & T. Kilian (Hrsg.). *Web 2.0 Neue Perspektiven für Marketing und Medien*. Berlin, Heidelberg: Springer, 3–22.

Kim, H.-W., Xu, Y. & Koh, J. (2004). A Comparison of Online Trust Building Factors between Potential Customers and Repeat Customers. *Journal of the Association for Information Systems*: 5 (10), 13.

Kim, J. & Moon, J. Y. (1998). Designing towards emotional usability in customer interfaces – trustworthiness of cyber-banking system interfaces. *Interacting with Computers, 10*, 1–29.

Kim, K. K. & Prabhakar, B. (2002). Initial trust and the adoption of B2C e-commerce: The case of internet banking. *ACM SIGMIS Database,* 35 (2), 50-64.

Kimmel, A. J. (2010). *Connecting With Consumers: Marketing For New Marketplace Realities.* New York: Oxford University Press.

Kohli, A. K. & Bernard J. J. (1990). Market Orientation: The Construct, Research Propositions, and Managerial Implications. *Journal of Marketing, 54*, 1–18.

Kohli, R., Devaraj, S. & Mahmood, A. (2004). Understanding Determinants of Online Consumer Satisfaction: A Decision Process Perspective. *Journal of Management Information Systems*, 21 (1), 115–135.

Kornblum, J. (2007). Online privacy? For young people, that's old-school. *USA Today*. Gefunden am 19. Oktober 2009 unter www.usatoday.com/tech/webguide/internetlife/2007-10-22-online-privacy_N.htm

Kotler, P. & Bliemel, F. (2001). Marketing-Management. Analyse, Planung, Umsetzung und Steuerung. 7. Auflage. Stuttgart: Schäffer-Poeschel Verlag.

Kotler, P. (1972). A Generic Concept of Marketing. *Journal of Marketing* 36 (2), 46–54.

Kotler, P. (2011). E-Mail-Austausch vom 16.05.2011.

Kotler, P., Armstrong, G., Saunders J. & Wong, V. (2003). *Grundlagen des Marketing*. (3. Auflage). München: Pearson.

Koufaris, M. & Hampton-Sosa, W. (2004). The development of initial trust in an online company by new customers. *Information & Management*, 41 (3), 377–397.

Kovar, S. E., Burke K. G. & Kovar B. R. (2000). Consumer responses to the CPA WebTrustTM assurance. *Journal of Information Systems, 14*, 17–35.

Kramer, R. M. (1999). Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual Review of Psychology*, 50, 569–598.

Krasnova, H., Spiekermann, S., Koroleva K. & Hildebrand T. (2010). Online social networks: why we disclose. *Journal of Information Technology (Palgrave Macmillan)*, 25 (2), 109–125.

Kremp, M. (2011, 7. Mai). Datenlecks. Sony-Kundendaten zeitweise im Web abrufbar. *Spiegel Online*. Gefunden am 14. Juni 2011 unter www.spiegel.de/netzwelt/games/0,1518,761227,00.html

Krishnamurthy, S. (2001). An Empirical Study of the Causal Antecedents of Customer Confidence in E-Tailers. *First Monday 6* (1). Gefunden am 06. Dezember 2010 unter www.131.193.153.231/www/issues/issue6_1/krishnamurthy/index.html

Krotz, F. (2009). Die Veränderung von Privatheit und Öffentlichkeit in der heutigen Gesellschaft. merz. medien + erziehung. 53 (8), 12–21. Gefunden am 13. Dezember 2012 unter http://www.mediaculture-online.de/fileadmin/bibliothek/krotz_privatheit/krotz_privatheit.pdf

Kruskal, W. H. & Wallis, W. A. (1952). Use of ranks in one-criterion variance analysis. *Journal of the American Statistical Association*, 47, 583–621.

Lambert, S. (2006). Do we need a "Real" Taxonomy of e-Business Models? *Flinders University School of Commerce Research Paper Series, 06-6*. Gefunden am 06. Dezember 2010 unter www.flinders.edu.au/shadomx/apps/fms/fmsdownload.cfm?file_uuid=FDBE4DE1-EB6B-7B71-0BCE-8FC142552687&siteName=sabs

Langer, W. (1999). *Einführung in die Grundlagen der explorativen Faktoranalyse*. Gefunden am 20. Oktober 2011 unter www.soziologie.uni-halle.de/langer/lisrel/skripten/faktorex.pdf

Langley, A. (2007). Process thinking in strategic organization. *Strategic Organization*, 5 (3), 271–282.

Lanier, C. D. & Saini, A. (2008). Understanding Consumer Privacy: A Review and Future Directions. *Academy of Marketing Science Review*, 12 (2). Gefunden am 06. Januar 2009 unter www.amsreview.org/articles/lanier02-2008.pdf.

Largo, R. H. (2011). *Baby Jahre*. Entwicklung und Erziehung in den ersten vier Jahren. (7. Auflage). München: Piper.

Laudon, K. & Traver, C. (2003). *E-commerce; business, technology, society*. Upper Saddle River, New Jersey: Pearson Prentice Hall.

Laufer, R. S. & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues, 33 (3)*, 438–458.

Lee, L. (2005, 25. August). Dell: In the Bloghouse. *BusinessWeek*. Gefunden am 06. April 2008 unter www.businessweek.com/technology/content/aug2005/tc20050825_2021.htm.

Lee, M. K. O. & Turban, E. (2001). A Trust Model for Consumer Internet Shopping. *International Journal of Electronic Commerce, 6* (1), 75–91.

Lenhart, A., Madden, M., Macgill, A. R. & Smith, A. (2007). *Teens and social media.* Washington, DC: Pew Internet & American Life Project. Gefunden am 25. August 2009 unter www.pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf .pdf

Leonhard, G. (2011). *Die Zukunft des Marketings. Daten – das neue Öl. MarketingJahrbuch* 2011 / 21. Jahrgang. R. Köhler (Hrsg.). St.Gallen: KünzlerBachmann Medien.

Lessig, L. (2002). Privacy as Property. *Social Research*, 69 (1), 247–269.

Lewicki, R. J. & Bunker, B. B. (1995). Trust in relationships: A model of development and decline. In: B. B. Bunker & J. Z. Rubin (Hrsg.). *Conflict cooperation and justice: Essays Inspired by the Work of Morton Deutsch*. San Francisco: Jossey-Bass, 133–173.

Lewis, K., Kaufman, J. & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal Of Computer-Mediated Communication*, 14 (1), 79–100.

Li, Ch. & Bernoff, J. (2008). *Groundswell: Winning in a World Transformed by Social Technologies*. Boston: Harvard Business Press.

Li, H., Sarathy, R. & Xu, H. (2010). Understanding Situational Online Information Disclosure as a Privacy Calculus. *Journal of Computer Information Systems*, 51 (1), 62–71.

Linder, J. C. & Cantrell, S. (2000). *Changing business models: surveying the landscape*. Accenture Institute for Strategic Change.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media Society, 10* (3), 393–411.

Luhmann, N. (1979). *Trust and Power.* Chichester: John Wiley & Sons.

Luhmann, N. (2000). *Vertrauen: ein Mechanismus der Reduktion sozialer Komplexität.* Stuttgart: Lucius und Lucius.

Luo, W. & Cook, D. (2007–2008). An empirical Study of Trust of Third Party Rating Services. *Journal of Computer Information Systems, 48* (2), 66–73.

Luo, X. (2002). Trust production and privacy concerns on the internet. A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management, 31*, 111–118.

Lwin, M. O. & Williams, J. D. (2003). A model integrating the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online. *Marketing Letters,* 14, 257–272.

Lynch, P. D., Kent, R. J. & Srinivasan, S. S. (2001). The global internet shopper: Evidence from shopping tasks in twelve countries. *Journal of Advertising Research*, 41 (3), 15–23.

Magretta, J. (2002). Why Business Models Matter. *Harvard Business Review*, 80, 86–92.

Mahadevan, B. B. (2000). Business Models for Internet-Based E-Commerce: An Anatomy. *California Management Review*, 42 (4), 55–69.

Marwick, A. E., Diaz, D. & Palfrey, J. G. (2010). Youth, Privacy and Reputation (Literature Review). Berkman Center Research Publication No. 2010-5; Harvard Public Law Working Paper No. 10–29.

Mason, R. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly, 10* (1), 5–12.

Mayer, R. C., Davis J. H. & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review,* 20 (3), 709–734.

Mayring, P. (1991). Qualitative Inhaltsanalyse. In: U. Flick, E. v. Kardorff, H. Keupp, L. v. Rosenstiel & S. Wolff (Hrsg.). *Handbuch qualitative Sozialforschung. Grundlagen, Konzepte, Methoden und Anwendungen*. München: Psychologie Verlags Union, 517.

Mayring, P. (2002). *Einführung in die Qualitative Sozialforschung*. Weinheim: Beltz.

McAllister, D. J. (1995). Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of management Journal, 38* (1), 24–59.

McKnight, D. H. & Chervany, N. L. (2002). What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce, 6* (2), 35–59.

McKnight, D. H., Choudhury, V. & Kacmar, C. J. (2000). Trust in e-commerce vendors: A two-stage model. *ICIS '00 Proceedings of the twenty first international conference on Information systems*. Atlanta: ACM Press, 532–536.

McKnight, D. H., Choudhury, V. & Kacmar, C. J. (2002a). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research, 13* (3), 334–359.

McKnight, D. H., Choudhury, V. & Kacmar, C. J. (2002b). The Impact of Initial Consumer Trust on Intentions to Transact with a web site: a trust building Model. *Journal of Strategic Information Systems, 11*, 297–323.

McKnight, D. H., Kacmar, C. J. & Choudhury, V. (2004). Dispositional trust and distrust distinctions in predicting high and low-risk Internet expert advice site perceptions. *e-Service Journal*, 3 (2), 35–58.

McKnight, D., Cummings, L. L. & Chervany, N. L. (1998). Initial Trust Formation in new Organizational Relationships. *Academy Of Management Review*, 23 (3), 473–490.

Meckel, M. & Lyczek, B. (2008). Corporate Communications als integraler Wertschöpfungsprozess. Die neuen Kommunikationsfunktionen. *Marketing Review St. Gallen* 1, 9–13.

Meckel, M. (2008a). Reputationsevangelisten und Reputationsterroristen. Unternehmenskommunikation 2.0. In: M. Meckel & K. Stanoevska-Slabeva (Hrsg.). *Web 2.0 – Die nächste Generation Internet*. Baden-Baden: Nomos Verlagsgesellschaft.

Meckel, M. (2008b). Unternehmenskommunikation 2.0 – ein Paradigmenwechsel? In: M. Meckel & B.F. Schmid (Hrsg.). *Unternehmenskommunikation. Kommunikationsmanagement aus Sicht der Unternehmensführung*. (2. Auflage,). Wiesbaden: Gabler, 473–492.

Meckel, M. (2011). *Next. Erinnerungen an eine Zukunft ohne uns*. Reinbeck: Rowohlt.

Meffert, H. (1986). Marketing. Grundlagen der Absatzpolitik. Wiesbaden.

Mesch, G. S. & Beker, G. (2010). Are Norms of Disclosure of Online and Offline Personal Information Associated with the Disclosure of Personal Information Online? *Human Communication Research*, 36 (4), 570–592.

Metzler, M. (2012, 16. September). Private Datensammlung als gefährliche Goldgrube. *NZZ am Sonntag*.

Meuser, M. & Nagel, U. (1991). ExpertInneninterviews – vielfach erprobt, wenig bedacht. Ein Beitrag zur qualitativen Methodendiskussion. In: D. Garz & K. Kraimer (Hrsg.). *Qualitativ-empirische Sozialforschung*. Opladen: Leske und Budrich, 441–471.

Meyer, R. (2011). *Datenschutzzertifikate – hoher Aufwand, hoher Nutzen?* Marketing 2011 / 21. Jahrgang. R. Köhler (Hrsg.). St. Gallen: KünzlerBachmann Medien.

Migipedia. (2012). Startseite von Migipedia. Gefunden am 11. März 2012 unter www.migipedia.ch/de/

Mills, J. L. (2008). *Privacy: the lost right*. Oxford, England: Oxford University Press.

Milne, G. R. & Boza, M.-E. (1999). Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices. *Journal of Interactive Marketing, 13* (1), 5–24.

Milne, G. R. & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18* (3), 15–29.

Milne, G. R. & Gordon, M. E. (1993). Direct Mail Privacy-Efficiency Trade-offs Within an Implied Social Contract Framework. *Journal of Public Policy & Marketing, 12* (2), 206–215.

Milne, G. R. & Rohm, A. J. (2000). Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives. *Journal of Public Policy & Marketing, 19* (2), 238–249.

Milne, G. R. (1997). Consumer Participation in Mailing Lists: A Field Experiment. *Journal of Public Policy & Marketing, 16*, 298–309.

Milne, G. R. (2000). Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue. *Journal of Public Policy & Marketing, 19* (1), 1–6.

Milne, G. R., Culnan, M. J. & Greene, H. (2006). A Longitudinal Assessment of Online Privacy Notice Readability. *Journal of Public Policy & Marketing, 25* (2), 238–249.

Milne, G. R., Rohm, A. J. & Bahl, S. (2004). Consumer Protection of Online Privacy and Identity. *The Journal of Consumer Affairs, 38 (2)*, 217–232.

Misoch, S. (2004). Identitäten im Internet. *Selbstdarstellung auf privaten Homepages*. Konstanz: UVK.

Mittal, B. (1989). Measuring Purchase-Decision Involvement. *Psychology & Marketing*, 6 (2), 147–162.

Mittal, V. & Kamakura, W. A. (2001). Satisfaction, Repurchase Intent, and Repurchase Behavior: Investigating the Moderating Effect of Customer Characteristics. *Journal of Marketing Research (JMR)*, 38 (1), 131–142.

Miyazaki, A. D. & Fernandez, A. (2000). Internet Privacy and Security: An Examination of Online Retailer Disclosures. *Journal of Public Policy & Marketing, 19* (1), 54–61.

Mohr, J. & Spekman, R. (1994). Characteristics of Partnership success: Partnership Attributes, Communication Behavior, and Conflict Resolution Techniques. *Strategic Management Journal*, 15 (2), 135–152.

Montgomery, A. L. & Smith, M. D. (2009). Prospects for personalization on the internet. *Journal of Interactive Marketing, 23* (2), 130–137.

Montgomery, K. & Pasnik, S. (1996). *Web of deception: Threats to children from online marketing.* Washington, DC: Center for Media Education.

Moormann, C., Deshapande, R. & Zaltman, G. (1993). Factors Affecting Trust in Market Research Relationships. *Journal of Marketing*, 57 (1), 81–100.

Moreno, M. A., Vander Stoep, A., Parks, M. R., Zimmerman, F. J., Kurth, A. & Christakis, D. A. (2009). Reducing at-risk adolescents' display of risk behavior on a social networking Web site: a randomized controlled pilot intervention trial. *Archives of Pediatrics & Adolescent Medicine, 163* (1), 35–41.

Morgan, R. M. & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing, 58* (3), 20–38.

Morris, J. H. & Moberg, D. J. (1994). Work organizations as contexts for trust and betrayal. In: Sarbin, T. R., Carney, R. M. & Eoyang, C. (Hrsg.). *Citizen espionage: studies in trust and betrayal*. Westport, CT, 163–201.

Moscardelli, D. M. & Divine, R. (2007). Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships With Privacy-Protecting Behaviors. *Family and Consumer Sciences Research Journal, 35* (3), 232–252.

Moscardelli, D. M. & Liston-Heyes, C. (2004). Teens Surfing The Net: How Do They Learn To Protect Their Privacy? *Journal of Business and Economics Research, 2* (9), 43–56.

MyCare. (2012). *Datenschutz und AGBs bei MyCare*. Gefunden am 11. März 2012 unter www.mycare.de/datenschutz und www.mycare.de/agb

Nahapiet, J. & Ghoshal, S. (1998). Social Capital, Intellectual Capital, and the Organizational Advantage. *Academy Of Management Review*, 23 (2), 242–266.

Nash, E. (1993). *Database Marketing: The Ultimate Selling Tool*. New York: McGraw-Hill.

Nielsen, J. A. (1999). *Trust or bust: Communicationing trustworthiness in web design*. Gefunden am 27. Oktober 2009 unter www.useit.com/alertbox/990307.html

Nissenbaum, H. (2001). Securing Trust Online: Wisdom or Oxymoron? Boston University *Law Review, 81* (3), 101–131.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Palo Alto, California: Stanford University Press.

Nokia Siemens Networks. (2009). *Privacy Survey 2009*. Gefunden am 29. September 2010 unter www.nokiasiemensnetworks.com/news-events/press/press-releases

Norberg, P. A., Horne, D. R. & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs*, 41 (1), 100–126.

Nosko, A., Wood, E. & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in Human Behavior*, 26 (3), 406–418.

Nowak, G. & Phelps, J. (1995). Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When "Privacy" Matters. *Journal of Direct Marketing, 9* (3), 46–60.

Nowak, G. & Phelps, J. (1997). Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When 'Privacy' Matters. *Journal of Direct Marketing, 11* (4), 94–108.

Nowak, G. J. & Phelps, J. (1992). Understanding Privacy Concerns. *Journal of Direct Marketing, 6* (4), 28–39.

Nussbaum, E. (2007). Kids, the Internet, and the End of Privacy: The Greatest Generation Gap Since Rock and Roll. *New York Magazine*. Gefunden am 13. Oktober 2009 unter www.nymag.com/news/features/27341/

O'Donnell, S. (2002). *An Economic Map of the Internet.* TPRC 30th Research Conference on Communication, Information and Internet Policy, 29. September 2002, Alexandria, VA, USA.

O'Reilly, T. (2006). *Web 2.0 Compact Definition: Trying again.* Sebastopol: O'Reilly Media.

O'Reilly, T. (2007). What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. *Communications and Strategies, International Journal of Digital Economics, 65*, 17–37.

Oerter, R. & Montada, L. (2002). *Entwicklungspsychologie*. (5., vollständig überarbeitete Auflage). Weinheim: Beltz PVU.

Okazaki, S., Li, H. & Hirose, M. (2009). Consumer Privacy Concerns and Preference for Degree of Regulatory Control. *Journal of Advertising, 38* (4), 63–77.

Olivero, N. & Lunt, P. (2004). Privacy versus Willingness to Disclose in e-Commerce Exchanges: The Effect of Risk Awareness on the relative Role of Trust and Control. *Journal of Economic Psychology, 25* (2), 243–262.

Olson, J. S. & Olson, G. M. (2000). i2i TRUST IN E-COMMERCE. *Communications of the ACM, 43* (12), 41–44.

Orwell, G. (1948). *1984*. London: Secker and Warburg.

Osterwalder, A. & Pigneur, Y. (2002). *An e-Business Model Ontology for Modeling e-Business.* 15th Bled Electronic Commerce Conference e-Reality: Constructing the e-Economy, 17–19 Juni 2002, Bled, Slovenien.

Osterwalder, A. & Pigneur, Y. (2010). *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers*. New Jersey: Wiley.

Palfrey, J. & Gasser, U. (2008). *Born Digital: Understanding the First Generation of Digital Natives.* New York: Basic Books.

Palmer, J. W., Bailey, J. P. & Faraj, S. (2000). The role of intermediaries in the development of trust on the www: The use and prominence of trusted third parties and privacy statements. *Journal of Computer-Mediated Communication, 5* (3). Gefunden am 30. Dezember 2012 unter http://jcmc.indiana.edu/vol5/issue3/palmer.html

Parker, R. B. (1974). A Definition of Privacy. *Rutgers Law Review, 27* (2), 275–296.

Parship. (2012). *Wir haben uns gefunden bei Parship*. Gefunden am 11. März 2012 unter www.parship.ch/

Pavlou, P. (2002). Trustworthiness as a Source of Competitive Advantage in Online Auction Markets. *Academy of Management Proceedings, 1*, A1–A6.

Pealer, L. N., Weiler, R. M., Pigg, R. M., Miller, D. & Dorman, S. M. (2001). The feasibility of a web-based surveillance system to collect health risk behaviour form data from college students. *Health, Education and Behaviour, 28* (5), 547–599.

Pennington, R., Wilcox, H. D. & Grover, V. (2003). The Role of System Trust in Business-to-Consumer Transactions. *Journal of Management Information Systems, 20* (3), 197–226.

Peslak, A. R. (2005). An Ethical Exploration of Privacy and Radio Frequency Identification. *Journal of Business Ethics, 59* (4), 327–345.

Peterson, R. A. (1994). A meta-analysis of Cronbach's coefficient alpha. *Journal of Consumer Research*, 21 (2), 381–391.

Phelps, J. E., D'Souza, G. & Nowak, G. J. (2001). Antecedents and Consequences of Consumer Privacy Concerns: An empirical Investigation. *Journal of Interactive Marketing, 15* (4), 2–17.

Phelps, J., Nowak, G. & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing, 19* (1), 27–41.

Pleil, Th. (2005). Öffentliche Meinung aus dem Netz? Neue Internet-Anwendungen und Public Relations. In: K. Arnold, & Ch. Neuenberger (Hrsg.). Alte Medien neue Medien: Theorieperspektiven, Medienprofile, Einsatzfelder. Gefunden am 10. Dezember 2012 unter www.suk.h-da.de/fileadmin/dokumente/berichte-forschung/2005/Pleil_Internet_PR.pdf

Pollach, I. (2005). A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent. *Journal of Business Ethics, 62* (3), 221–235.

Porter, M. E. (2001). Strategy and the Internet. *Harvard Business Review,* 79 (3),73.

Posterjack. (2012). *Startseite Posterjack*. Gefunden am 11. März 2012 unter www.posterjack.ch

Premazzi, K., Castaldo, S., Grosso, M., Raman, P., Brudvig, S. & Hofacker, C. F. (2010). Customer Information Sharing with E-Vendors: The Roles of Incentives and Trust. *International Journal of Electronic Commerce*, 14 (3), 63–91.

Prensky, M. (2001). *Digital Natives, Digital Immigrants* Part 1. On the Horizon. 9 (5), 1–6.

Prosser, W. (1960). The Torts of Privacy. *California Law Review, 48* (3), 383–423.

Putnam, R. D. (1993). *Making Democracy Work. Civic Traditions in Modern Italy*. New Jersey: Princeton University Press.

Qureshi, I., Fang, Y., Ramsey, E., McCole, P., Ibbotson, P. & Compeau, D. (2009). Understanding Online Customer Repurchasing Intention and the Mediating Role of Trust –

An Empirial Investigation in Two Developed Countries. *European Journal of Information Systems,* 18 (3), 205–222.

Raghu, T. S., Kannan, P. K., Rao, H. R. & Whinston, A. B. (2001). Dynamic profiling of consumers for customized offerings over the Internet: A model and analysis. *Decision Support Systems, 32* (2), 117–134.

Raman, P. & Pashupati, T. K. (2005). Online privacy: the impact of self perceived technological competence. In: S. Krishnamurthy (Hrsg.). *Contemporary Research in E-Marketing, Volume 1*. Hershey, PA: Idea Group Inc., 200–225.

Rappa, M. A. (2004). The Utility Business Model and the Future of Computing Services. IBM *Systems Journal, 43* (1), 32–42.

Rappa, M. A. (2011). Managing the Digital Enterprise – Business Models of the Web. Gefunden am 11. September 2011 unter www.digitalenterprise.org/models/models.html

Ratnasingam, P. (1998). The Importance of Trust in Electronic Commerce. *Internet Research: Electronic Networking Applications and Policy*, 8 (4), 313–321.

Reinhold, G. (1997). *Interaktion*. In: G. Reinhold & S. Lamnek (Hrsg.). Reinhold Soziologie-Lexikon.). München: Oldenbourg, 305.

Renner, K. H., Schütz, A. & Machilek, F. (2005). Internet und Persönlichkeit: Stand der Forschung und Perspektiven. Gefunden am 17. August 2012 unter www.psydok.sulb.uni-saarland.de/volltexte/2006/582/pdf/pdf14.pdf

Ricardo. (2012). *Willkommen im gröööössten Shopping-Center der Schweiz*. Gefunden am 11. März 2012 unter www.ricardo.ch/

Richards, J. (1997). Legal Potholes on the Information Superhighway. *Journal of Public Policy & Marketing, 16*, 319–326.

Ridings, C. M., Gefen, D. & Arinze, B. (2002). Some antecedents and effects of trust in virtual communities. *The Journal of Strategic Information Systems, 11* (3–4), 271–295.

Riegelsberger, J. & Sasse, A. M. (2001). Trustbuilders and trustbusters. The role of trust cues in interfaces to e-commerce applications. *Proceedings of the 1st IFIP Conference on e-commerce, e-business, e-government, i3e,* 17–30. Zürich, Schweiz. Gefunden am 30.12.2012 unter www.cs.ucl.ac.uk/staff/j.riegelsberger/trustbuilders_and_trustbusters.htm

Riegelsberger, J., Sasse, A. M. & McCarthy, J. D. (2003). Shiny Happy People Building Trust? Photos on e-Commerce Websites and Consumer Trust. *Proceedings of the SIGCHI 2003 Conference on Human Factors in Computing System*. New York: ACM Press, 121–128.

Rinne, H. (2000). *Taschenbuch der Statistik*. Frankfurt am Main: Verlag Harri Deutsch.

Riordan, C. M., Gatewood, R. D. & Bill, J. B. (1997). Corporate Image: Employee Reactions and Implications for Managing Corporate Social Performance. *Journal of Business Ethics*, 16 (4), 401–412.

Rosen, E. (2009). *The Anatomy of Buzz Revisited: Real-life lessons in Word-of-Mouth Marketing*. New York: Doubleday.

Rosenbach, M. & Schmundt, H. (2011). Das perfekte Verbrechen. *Der Spiegel*, Nr. 27, 28–38.

Rössler, B. (2001). *Der Wert des Privaten*. Frankfurt/Main: Suhrkamp.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality*, 35, 651–665.

Rousseau, D., Sitkin, S. B., Burt, R. S. & Camerer, C. (1998). Not so different after all: A cross-discipline View of Trust. *Academy of Management Review, 23* (3), 393–404.

Ruisinger, D. (2007). *Online Relations. Leitfaden für moderne PR im Netz*. Stuttgart: Schäffer-Poeschel Verlag.

Rust, R. T., Kannan, P. K. & Peng, N. (2002). The Customer Economics of Internet Privacy. *Journal of the Academy of Marketing Science, 30* (4), 455–464.

Sako, M. (1998). *Does Trust Improve Business Performance?*. Trust within and between organizations: Conceptual issues and empirical applications. Oxford, New York: University Press. 88–117.

Salzlandkreis. (2012). *Support bei Salzlandkreis*. Gefunden am 11. März 2012 unter www.salzlandkreis.net/support/

Sandberg, K. D. (2002). Kicking the Tires of Corporate Reputation. *Harvard Management Communication Letter*, 5 (1), 3.

Sarathy, R. & Robertson, C. J. (2003). Strategic and Ethical Considerations in Managing Digital Privacy. *Journal of Business Ethics, 46* (2), 111–126.

Scanzoni, J. (1979). Social Exchange and Behavioral Interdependence. In: R. Burgess & T. Huston (Hrsg.). *Social Exchange in Developing Relationships.* New York: Academic Press.

Scheer, C., Deelamnn, T. & Loos, P. (2003). *Geschäftsmodelle und internetbasierte Geschäftsmodelle – Begriffsbestimmung und Teilnehmermodell*. Working Paper of the Research Group Information Systems & Management. Mainz: Johannes Gutenberg-University Mainz. Gefunden am 15. Dezember 2010 unter www.isym.bwl.uni-mainz.de/publikationen/isym012.pdf

Schlenker, B. R., Helm, B. & Tedeschi, J. T. (1973). The effects of personality and situational variables on behavioral trust. *Journal of Personality and Social Psychology*, 25, 419–427.

Schlosser, A. E., White, T. B. & Lloyd, S. M. (2006). Converting Web Site Visitors into Buyers: How Web Site Investment Increases Consumer Trusting Beliefs and Online Purchase Intentions. *Journal of Marketing, 70* (2), 133–148.

Schmidt, Ch. (2011, 23. Februar). Im Wandel der Zeit. Wie sich Online- und Versandhandel in Deutschland entwickelt haben und sich an die neuen technischen Möglichkeiten anpassen. *Frankfurter Allgemeine Zeitung*, Verlagsbeilage: Online- und Versandhandel, Nr. 45, B3.

Schmundt, H. (2011, 2. Mai). Datenschutz. Fund im Sternbild Krake. *Der Spiegel*, 18/2011. 116–118.

Schoenbachler, D. D. & Gordon, G. L. (2002). Trust and Customer Willingness to provide Information in Database-driven Relationship Marketing. *Journal of Interactive Marketing, 16* (3), 2–16.

Schulz, S., Büttner, O. B. & Silberer, G. (2008). Vertrauen und Vertrauenswürdigkeit im Internet am Beispiel von Internetapotheken. In: A. Gröppel-Klein & C. C. Germelmann (Hrsg.). *Medien im Marketing: Optionen der Unternehmenskommunikation*. Wiesbaden: Gabler, 473–492.

Schuppisser, R. (2012, 12. August). Der Schlüssel zum besseren Menschen. Im Internet bezahlen wir mit unseren Daten. Das macht die Gesellschaft transparenter und womöglich auch besser. *Der Sonntag*, 37.

Schurter, D. (2011, 26. Mai). Verheiratet? 2 Cents! iPhone? 3 Cents! *20 Minuten Online*. Gefunden am 26. Mai 2011 unter www.20min.ch/digital/webpage/story/28271517

Seidler, Ch. (2009, 18. Oktober). Datenpanne drängt SchülerVZ in die Defensive. *Spiegel Online.* Gefunden am 05. Januar 2010 unter www.spiegel.de/netzwelt/netzpolitik/0,1518,655820,00.html.

Sen, R. (2005). Optimal Search Engine Marketing Strategy. International Journal Of Electronic Commerce, 10 (1), 9–25.

Shankar, V., Smith, A. K. & Rangaswamy, A. (2003). Customer satisfaction and loyalty in online and offline environments. *International Journal of Research in Marketing, 20* (2), 153–175.

Shankar, V., Urban, G. L. & Sultan, F. (2002). Online Trust: A Stakeholder Perspective, Concepts, Implications, and Future Directions. *Journal of Strategic Information Systems, 11* (3–4), 325–344.

Shaw, E. H. & Jones, D. (2005). A history of schools of marketing thought. *Marketing Theory*, 5 (3), 239–281.

Sheehan, K. B. & Hoy, M. G. (1999). Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. *Journal of Advertising, 28* (3), 37–51.

Sheehan, K. B. & Hoy, M. G. (2000). Dimensions of Privacy Concern Among Online Consumers. *Journal of Public Policy & Marketing, 19* (1), 62–73.

Sheehan, K. B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing, 13* (4), 24–38.

Shneiderman, B. (2000). Designing Trust into Online Experiences. *Communications of the ACM, 43* (12), 57–59.

Siegrist, M. (2000). The Influence of Trust and Perceptions of Risks and Benefits on the Acceptance of Gene Technology. *Risk Analysis, 20* (2), 195–204.

Siegrist, M., Gutscher, H. & Earle, T. C. (2005). Perception of risk: the influence of general trust, and general confidence. *Journal of Risk Research, 8* (2), 145–156.

Sitkin, S. B. & Roth, N. L. (1993). Explaining the limited effectiveness of legalistic "remedies" for trust / distrust. *Organization Science*, 4, 367–392.

Smith, D., Menon, S. & Sivakumar, K. (2005). Online peer and editorial recommendations, trust, and choice in virtual markets. *Journal of Interactive Marketing, 19* (3), 15–37.

Smith, H. J., Milberg, S. J. & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly, 20* (2), 167–196.

Smith, R. E. (2002). *Compilation of State and Federal Privacy Laws*. Washington DC: Privacy Journal.

Solomon, M. R. (2004). Consumer behavior: buying, having, and being. (6. Auflage). Upper Saddle River: Prentice Hall.

Solove, D. J. & Schwartz, P. M. (2009). *Information Privacy Law.* (6. Auflage). New York: Aspen Publishers.

Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review, 90*, 1087–1155.

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York: NYU Press.

Solove, D. J. (2005). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154* (3), 477–560.

Solove, D. J. (2007). *The future of reputation: gossip, rumor, and privacy on the Internet.* New Haven/London: Yale University Press.

Soltani, A. (2011, 13. Mai). *Your Marital Status Is Worth $0.01 To Data-Buyers, Your Smartphone Is Worth $0.03.* Kashmir Hill. The Not-So Private Parts. Gefunden am 26. Mai 2011 unter www.blogs.forbes.com/kashmirhill/2011/05/13/your-marital-status-is-worth-0-01-to-data-buyers-your-smartphone-is-worth-0-03/

Speier, C., Harvey, M. & Palmer, J. (1998). Virtual management of global marketing relationships. *Journal of World Business, 33* (3), 263–276.

Spiegel Online. (2010, 16. Oktober). Nutzer kopiert massenhaft „SchülerVZ"-Profile. *Spiegel Online.* Gefunden am 05. Januar 2010 unter www.spiegel.de/netzwelt/netzpolitik/0,1518,655703,00.html

Sprenger, P. (1999, 26. Januar). Sun on Privacy: "Get over it". *Wired.com*. Gefunden am 26. September 2009 unter www.wired.com/politics/law/news/1999/01/17538

Standifird, S.S. (2001). Reputation and e-commerce: eBay auctions and the asymmetrical impact of positive and negative ratings. *Journal of Management*, 27, 279-295.

Starbucks. (2012). *My Starbucks Idea.* Gefunden am 11. März 2012 unter www.mystarbucksidea.force.com/

Steeves, V. & Webster, C. (2008). Closing the barn door: the effect of parental supervision on Canadian children's online privacy. *Bulletin of Science, Technology & Society, 28*(1), 4-19.

Steeves, V. & Wing, C. (2005). *Young Canadians in a wired world phase II: Trends and recommendations.* Ottawa, ON: Media Awareness Network.

Stewart, D.W. (1981). The application and misapplication of factor analysis in marketing research. *Journal of Marketing Research*, 18(1), 51-62.

Stewart, K.A. & Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research, 13*(1), 36-49.

Stolz, C.D. (2008). *Erfolgsmessung Informationsorientierter Websites*. Norderstedt: Books on Demand.

Stratenschulte, J. (2011, 9. Dezember). Google+. Facebook-Rivale startet automatische Gesichtserkennung. Focus Online. Gefunden am 02. Januar 2012 unter www.focus.de/digital/internet/google/internet-find-my-face-google-mit-gesichtserkennung-bei-fotos_aid_692362.html

Ström, P. (2006). *Die Überwachungsmafia. Das lukrative Geschäft mit unseren Daten*. München: Wilhelm Heyne.

Tan, Y.-H. & Thoen, W. (2002). Formal aspects of a generic model trust for electronic commerce. *Decision Support Systems, 33* (3), 233–246.

Tapscott, D., Ticoll, D. & Lowy, A. (2000). *Digital Capital: Harnessing the Power of Business Webs.* Boston: Harvard Business School Press.

Taraszow, T., Aristodemou, E., Shitta, G., Laouris, Y. & Arsoy, A. (2010). Disclosure of personal and contact information by young people in social networking sites: An analysis using Facebook™ profiles as an example. *International Journal of Media & Cultural Politics*, 6 (1), 81–101.

Telekom. (2012). *Telekom hilft auf Twitter*. Gefunden am 11. März 2012 unter www.twitter.com/#!/telekom_hilft

Theobald, A. (2001). Sinn und Unsinn von Incentives in der Online-Marktforschung. In: A. Theobald, M. Dreyer & T. Starsetzki (Hrsg.). *Online Marktforschung: Theoretische Grundlagen und praktische Erfahrungen*. Wiesbaden: Gabler, 395–407.

Timmers, P. (1998). Business Models for Electronic Markets. *Electronic Markets, 8* (2), 3–8.

Timmers, P. (2000). *Electronic Commerce. Strategies and Models for Business-to-Business Trading*. West Sussex: Wiley.

Tucker, A. W. & Kuhn, H. W. (1950). Contributions to the theory of games. *Annals of Mathematical Studies, volume II (28)*. Princeton: Princeton University Press.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28* (1), 20–36.

Turkle, S. (1995). *Life on the screen: Identity in the age of Internet*. New York: Simon & Schuster.

Turkle, S. (1998). *Leben im Netz. Identitäten in Zeiten des Internet*. Reinbek: Rowohlt.

Überla, K. (1977). *Faktorenanalyse. Eine systematische Einführung für Psychologen, Mediziner, Wirtschafts- und Sozialwissenschaftler*. Berlin: Springer-Verlag.

Urban, G. L., Amyx, C. & Lorenzon, A. (2009). Online Trust: State of the Art, New Frontiers, and Research Potential. *Journal of Interactive Marketing, 23* (2), 179–190.

Urban, G. L., Sultan, F. & Qualls, W. J. (2000). Placing Trust at the Center of Your Internet Strategy. *Sloan Management Review, 42* (1), 39–48.

van Den Haag, E. (1971). On Privacy. In: J. R. Pennock & J. W. Chapman (Hrsg.). *Nomos XIII*. New York: Atherton Press, 147–153.

van den Poel, D. & Leunis, J. (1999). Consumer Acceptance of the Internet as a Channel of Distribution. Journal of Business Research, 45 (7/3), 249–256.

van Eimeren, B. & Frees, B. (2009). *Der Internetnutzer 2009 – multimedial und total vernetzt?* Ergebnisse der ARD/ZDF-Onlinestudie 2009. media perspektiven 7/2009. Gefunden am 10. Dezember 2012 unter www.media-perspektiven.de/uploads/tx_mppublications/Eimeren1_7_09.pdf

van Riel, C. B. M. & Fombrun, C. J. (2007). *Essentials of Corporate Communication: Implementing Practices for Effective Reputation Management*. New York: Routledge.

Venkatesh, V. & Morris, M. (2000). Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS Quarterly*, *24* (1), 115–139.

Venkatesh, V. (2000). Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model. *Information Systems Research*, *11* (4), 342–365.

Vidmar, N. & Flaherty, D. H. (1985). Concern for Personal Privacy in an Electronic Age. *Journal of Communication, 35* (2), 91–103.

Volokh, E. (2000). Personalization and Privacy. Communications of the ACM, 43 (8), 84–88.

Wakefield, R. & Whitten, D. (2006). Examining User Perceptions of Third-Party Organization Credibility and Trust in an E-Retailer. *Journal of Organizational & End User Computing, 18* (2), 1–19.

Walczuch, R. & Lundgren, H. (2004). Psychological Antecedents of institution-based Consumer Trust in e-Retailing. *Information & Management, 42* (1), 159–177.

Wang, P. & Petrison, L. A. (1993). Direct Marketing Activities and Personal Privacy. *Journal of Direct Marketing, 7* (1), 7–19.

Wang, S., Beatty, S. E. & Foxx, W. (2004). Signaling the trustworthiness of Small Online Retailers. *Journal of Interactive Marketing, 18 (1)*, 53–69.

Warren, S. D. & Brandeis, L. (1890). The Right to Privacy. Harvard Law Review, 4 (5), 193–220. Gefunden am 05. Februar 2012 unter www.groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Wazlawik, P., Beavin, J. H. & Jackson, D. D. (1969). *Menschliche Kommunikation – Formen, Störungen, Paradoxien*. Huber: Bern.

Weill, P. & Vitale, M. R. (2001). *Place to Space: Migrating to eBusiness Models*. Boston: Harvard Business School Press.

Weinberger, D. (2000). The Longing. In: D. Weinberger, R. Levine, Ch. Locke & D. Searls (Hrsg.). *The Cluetrain Manifesto. The end of business as usual.* New York: Perseus.

Wemakeit (2012). *Startseite We make it*. Gefunden am 11. März 2012 unter www.wemakeit.ch/

Westin, A. F. (2003). Social and political dimensions of privacy. *Contemporary Perspectives on Privacy: Social, Psychological, Political, 59* (2), 431–453.

Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum Press.

Wheeless, L. R. & Grotz, J. (1976). Conceptualization and Measurement of Reported Self-disclosure. *Human Communication Research,* 2 (4), 338–346.

Wiedemann, P. (1994). *Krisenmanagement & Krisenkommunikation. Arbeiten zur Risiko-Kommunikation.* In: H. J. Uth (Hrsg.). Krisenmanagement bei Störfällen in Chemieanlagen. Berlin: Springer. Gefunden am 30. Dezember 2012 unter http://www2.fz-juelich.de/inb/inb-mut/publikationen/hefte/heft_41.pdf

Wilhelm, S. (2012). *E-Commerce-Umsatz erstmals mehr als 20 Milliarden Euro.* Der Handel. Ausgabe 4/2012. Gefunden am 22. April 2012 unter www.derhandel.de/news/technik/pages/E-Commerce-E-Commerce-Umsatz-erstmals-mehr-als-20-Milliarden-Euro-8293.html

Wilson, C. E. (1981). A Procedure for the Analysis of Consumer Decision Making. *Journal of Advertising Research*, 21 (2), 31–36.

Winer, R. S. (2001). A framework for customer relationship management. *California Management Review, 43* (4), 89–105.

Winkler, J. (2007). *Suchmaschinenoptimierung*. Poing: Franzis.

Wirtz, B. (2002). *Electronic Business*. Wiesbaden: Gabler.

Witte, J. & Reissmann, O. (2011, 03. Juni). Kundendaten kopiert. Hacker verhöhnen Sony mit neuer Attacke. *Spiegel Online*. Gefunden am 14. Juni 2011 unter www.spiegel.de/netzwelt/web/0,1518,766349,00.html

Witzel, A. (1982). *Verfahren der qualitative Sozialforschung. Überblick und Alternativen*. Frankfurt: Campus.

Wu, G., Hu, X. & Wu, Y. (2010). Effects of perceived interactivity, perceived web assurance and disposition to trust on initial online trust. *Journal of Computer-Mediated Communication*, 16 (1), 1–26.

Xie, E., Teo, H. & Wan, W. (2006). Volunteering personal information on the Internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. *Marketing Letters, 17* (1), 61–74.

Xing (2012). *Startseite und Privatsphäre Einstellungen bei Xing*. Gefunden am 11. März 2012 unter www.xing.com/

Yamagishi, T. & Yamagishi, M. (1994). Trust and commitment in the United States and Japan. *Motivation and Emotion*, 18, 129–166.

Yen, H. J. R. & Gwinner, K. P. (2003). Internet Retail Customer Loyalty: The Mediating Role of Relational Benefits. *International Journal of Service Industry Management, 14*, 483–500.

Yoon, S.-J. (2002). The Antecedents and Consequences of Trust in Online-Purchase Decisions. *Journal of Interactive Marketing, 16 (2)*, 47–63.

Youn, S. (2005). Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach. *Journal of Broadcasting & Electronic Media, 49* (1), 86–110.

Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs, 43* (3), 389–418.

Zalando. (2012). *Startseite Zalando*. Gefunden am 11. März 2012 unter www.zalando.ch/

Zhang, Y., Wang, C. L. & Chen, J. (2000). Consumers' responses to web-based data collection efforts and factors influencing the responses. *Journal of International Marketing and Market Research*, 25, 115–123.

Zhou, M. & Tian, D. (2010). An Integrated Model of Influential Antecedents of Online Shopping Initial Trust: Empirical Evidence in a Low-Trust Environment. *Journal of International Consumer Marketing,* 22 (2), 147–167.

Zimmer, D. (2010, 25. Oktober). Wenn Web Händler Offline gehen. Gefunden am 19. April 2011 unter www.internetworld.de/Heftarchiv/2010/Ausgabe-22-2010/Wenn-Web-Haendler-offline-gehen

Zündorf, L. (1986). Macht, Einfluss, Vertrauen und Verständigung. Zum Problem der Handlungskoordinierung in Arbeitsorganisationen. In: R. Seltz, U. Mill & E. Hildebrandt. (Hrsg.). Organisation als soziales System. Berlin: Sigma, 33–65.

Zureik, E. & Harling Stalker, L. L. (2010). *The cross-cultural study of privacy*. In: E. Zureik, L. L. Harling Stalker, E. Smith, D. Lyon, & Y. E. Chan. (Hrsg.). Surveillance, Privacy and The Globalization of Personal Information. Montreal: McGill-Queen's University Press, 8–30.

Zwick, D. & Dholakia, N. (2004). Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing. *Journal of Macromarketing, 24* (1), 31–43.

7 Anhang

7.1 Anhang zum Literaturteil

7.1.1 Übersicht über Geschäftsmodelldefinitionen mit Klassifizierung

Die untenstehende Tabelle beinhaltet einen Überblick über die in der Geschäftsmodellliteratur diskutierten Definitionen, die Kategorienbildung und ihre Differenzierungskriterien. Zusätzlich wurden die Beiträge der Autoren anhand ihrer Verbreitung in der akademischen Literatur bewertet, was anhand der Anzahl Zitationen nach „Google Scholar“[56] erfolgte (siehe eckige Klammern nach der Definition).

Autor, Publikationsjahr & Definitionsbezug	Definition & Anzahl Zitationen auf Google am 20.02.2012	Kategorienbildung	Differenzierungskriterium
Applegate (2000) Business Model	“A description of a complex business that enables study of its structure, the relationships among structural elements, and how it will respond in the real world” (S. 53). [75]	**Vier Kategorien:** Focused Distributor Models, Portal Models, Producer Models, Infrastructure Provider Models	Kein erkennbares Differenzierungskriterium
Afuah & Tucci (2001) Business Model	“Business Models is a method by which a firm builds and uses its resources to offer its customers better value than its competitors and to make money doing so” (S. 3). [929]	Keine eigenen Kategorien	Kein erkennbares Differenzierungskriterium
Bambury (1998) E-Commerce	“The term Electronic Commerce should be understood to include the conduct of business with the assistance of telecommunications and information technology; it is not limited to business conducted on the Internet.” [81]	**Zwei Kategorien & 15 Subkategorien:** Translated Real-World Business Models, Native Internet Business Models	Kein erkennbares Differenzierungskriterium
Betz (2002) Business Model	“A Business model is an abstraction of a business identifying how [it] profitably makes money” (S. 21). [63]	**Sechs Kategorien:** Strategic Finance, Strategic Enterprise, Strategic Response, Strategic Learning, Strategic Innovation, Strategic Firm	Ressourcen, Umsatz, Gewinn & Kapital
Eisenmann	A Business model is “a hypothesis about how a	**Acht Kategorien:** Internet Ac-	Kein erkennbares

[56] Stichtag: 20. Februar 2012.

(2002) Business Model	company will make money over the long term: what the company will sell, and to whom; how the company will collect revenue; what technologies it will employ; when it will rely on partners; and, following from the last two points, how its costs will 'scale' with growth" (S. xii). [102]	cess Providers, Online Portals, Online Content Providers, Online Retailers, Online Brokers, Online Market Makers, Networked Utility Providers, Application Service Providers	Differenzierungskriterium
Jones, Wilikens, Morris & Masera (2000) E-Business	"eBusiness is the carrying out of business activities that lead to an exchange of value, where the parties interact electronically, using network or telecommunications technologies" (S. 81). [160]	Keine eigenen Kategorien	Kein erkennbares Differenzierungskriterium
Laudon & Traver (2003) Business Model	"A business model is a set of planned activities (sometimes referred to as business processes) designed to result in a profit in a marketplace" (S. 61). [355]	**Sieben Kategorien:** Portal, E-Tailer, Content Provider, Transaction Broker, Market Creator, Service Provider, Community Provider	Kein erkennbares Differenzierungskriterium
Linder & Cantrell (2000) Business Model	"Business models are 'models' of an organization's core logic for creating value." [178]	**Acht Kategorien & 34 Subkategorien:** Price Model, Convenience Model, Commodity-plus Model, Experience Model, Channel Model, Intermediary Model, Trust Model, Innovation Model	Kernprofittätigkeit & relative Position im Preis / Wert Kontinuum
Mahadevan (2000) Business Model	"A business model is a unique blend of three streams that are critical to the business. These include the value stream for the business partners and the buyers, the revenue stream and the logistical stream. Value stream identifies the value proposition for the buyers, sellers and the market makers and portals in an Internet context. The revenue stream is a plan for assuring revenue generation for the business and the logistical stream addresses various issues related to the design of a supply chain for the business" (S. 55 - 69). [528]	**Drei Kategorien:** Portal, Market Makers, Product/Service Providers	Kein erkennbares Differenzierungskriterium
Osterwalder & Pigeur (2002) E-Business	"A business model is nothing else than a description of the value a company offers to one or several segments of customers and the architecture of the firm and its network of partners for creating, marketing and delivering this value and relationship capital, in order to generate profit-able and sustainable revenue streams" (S. 2). [351]	**Vier Kategorien:** Product Innovation, Infrastructure Management, Customer Relationship, Financial Aspects	Ertrag, Mehrwert & Kosten
Rappa (2011) Business Model	"A business model is the method of doing business by which a company can sustain itself -- that is, generate revenue." [176]	**Neun Kategorien & 41 Subkategorien:** Brokerage, Advertising Model, Infomediary Model, Merchant Model, Manufacturer Model, Affiliate Model, Community Model, Subscription Model, Utility Model	Kein erkennbares Differenzierungskriterium
Tapscott, Ticoll & Lowy (2000) E-Business	"Based on the Internet, fundamentally new [business] models of the firm and its interaction with external entities have emerged. Industry by industry these new Net-enabled models are destroying the old models of wealth creation. Call the new model of wealth the Business Web. A B-Web is an elaborate network of suppliers, distributors, commerce services providers, and customers that conduct business communications and transactions on the Internet and other electronic media in order to produce value for end-customers and for one another" (S. 198). [641]	**Fünf Kategorien:** Agora, Aggregation, Value Chain, Alliance, Distributive Network	Grad der ökonomischen Kontrolle & Grad der Wertschöpfungsintegration
Timmers (1998)	"An architecture for the product, service and information flows, including a description of the	**Elf Kategorien:** E-Shop, E-Procurement, E-Malls, E-	Innovationsgrad & Funktionale In-

Business Model	various business actors and their roles; and a description of the potential benefits for the various business actors; and a description of the sources of revenues" (S. 4). [1'321]	Auctions, Virtual Communities, Collaboration Platforms, Third-Party Marketplaces, Value-Chain Integrators, Value-Chain Service Provider, Information Brokerage, Trust Services	tegration
Weill & Vitale (2001) E-Business	"The essence of the way e-business is conducted. There are a finite number of atomic e-business models, which are building blocks of more complex business models. Each atomic e-business model is described by four characteristics: strategic objectives, sources of revenue, critical success factors, and core competencies required." [464]	**Acht Kategorien:** Content Provider, Direct to Customer, Full-Service Provider, Intermediary, Shared Infrastructure, Value Net Integrator, Virtual Community, Whole-of Enterprise	Strategische Zielsetzung, Quellen der Wertschöpfung, kritische Erfolgsfaktoren & Kernkompetenzen

7.1.2 Definition der elf Kategorien von Geschäftsmodellen nach Timmers (1998; 2000)

E-Shop	E-Shops sind Internetauftritte von Firmen, auf denen Güter und Dienstleistungen zum Verkauf angeboten werden, auf denen die Produkte oder Dienstleistungen meistens sogleich bestellt und bezahlt werden können. Der Medienanbieter exlibris.ch ist ein typischer Vertreter dieses Geschäftsmodells. Timmers (2000) beschreibt elektronische Shops als das Web-Marketing einer Firma, da die Webseite die Güter und Dienstleistungen der Firma bewirbt und anpreist. Der Grossteil der E-Shops ist im Business-to-Consumer- (B2C-) oder im Business-to-Business- (B2B-) Segment tätig. Im Unterschied zu real existierenden Shops ist es dem Verkäufer und dem Käufer prinzipiell immer möglich, anwesend zu sein, es gibt weder zeitliche noch örtliche Limitationen. Selten fallen bei E-Shops Bezahlung und Lieferung der Güter oder Dienstleistungen zusammen. Durch diesen zeitlich verschobenen Leistungsaustausch kann das Risiko des zuerst leistenden Vertragsteilnehmers erhöht werden (Standifird, 2001).
E-Procurement	E-Procurement umfasst die elektronische Beschaffung von Gütern und Dienstleistungen über das Internet, also eine Automation des Beschaffungsprozesses durch IT-Lösungen. Grösstenteils handelt es sich um geschlossene Netzwerke im B2B-Bereich, die die Vermittlung von Angebot und Nachfrage in der betrieblichen Beschaffung unterstützen. Als Vorteile von E-Procurement führt Timmers (2000) Kosten- und Zeitersparnisse, verbesserte Qualität, schnellere Lieferzeiten und günstigeres Beschaffungsmanagement auf. Da bei E-Procurement die Schnittstellenkompatibilität gewährleistet sein muss, lohnt sich ein gemeinsames System nur, wenn der Beschaffungsumfang hoch ist und regelmässig erfolgt (Andressen, 2010; Weill & Vitale, 2001), wie dies zum Beispiel bei Japan Airlines der Fall ist. E-Procurement ist ein Geschäftsmodell, welches durch Kostenersparnisse und nicht durch Umsatz legitimiert wird.
E-Mall	Eine E-Mall ist eine Ansammlung von E-Shops, meistens unter einem gemeinsamen Nenner (zum Beispiel einem Marktsegment) oder einer gemeinsamen Marke, vergleichbar mit einem Einkaufszentrum in der realen Welt. Ein Beispiel ist das Internetkaufhaus Netzmarkt. Meistens bietet der E-Mall-Anbieter gemeinsame Zahlungsabwicklung und einen einheitlichen Transportservice an, was zur Kostenreduktion der E-Shops führt. Der Anbieter dieses B2B-Geschäftsmodells unterstützt Anbieter von E-Shops gegen eine Gebühr mit technischen Lösungen und Dienstleistungen. Ausserdem sieht das Geschäftsmodell den Verkauf von Werbeplätzen vor (Timmers, 2000; Balocco, Rangone, Cardano & Valacca, 2004).
E-Auction	Elektronische Auktionen sind Versteigerungen von Produkten oder Dienstleistungen auf einer Online-Plattform des E-Auction-Anbieters. Der Versteigerer (Business oder Consumer) bietet sein Angebot zu einem Preis an und der Ersteigerer (Business oder Consumer) kann innerhalb festgelegter Rahmenbedingungen öffentlich sichtbar seine Angebote abgeben. Bei normalen Auktionen erhält der Meistbietende nach Ablauf der Versteigerungszeit den Zuschlag. Der Plattformanbieter stellt dem Versteigerer die Plattform gegen Entrichtung von Nutzungsgebühren zur Verfügung und kann die Seite bei hohen Besucherzahlen auch gut als Werbeplattform positionieren (Mahadevan, 2000; Timmers, 2000). Bekannte Auktionshäuser sind zum Beispiel eBay oder Ricardo.
Virtual Community	Ridings, Gefen und Arinze (2002) definieren virtuelle Communitys als einen Zusammenschluss von Menschen mit gleichen Interessen, welche sich regelmässig über das Internet austauschen. Einer der grössten Vorteile von virtuellen Communitys ist, dass durch das Internet Distanz- und Zeitbarrieren überwunden werden können, welche in traditionellen Communitys bestehen. Nach Hagel und Armstrong (1997) befriedigen virtuelle Communitys folgende vier Kundenbedürfnisse: Ressourcen teilen, Beziehungen etablieren, Güter oder Informationen handeln und Fantasien ausleben. Der Erfolg von virtuellen Communitys beruht darauf, dass dessen Mitglieder bereit sind, Zeit und Aufwand für ihre Partizipation an der Community zu investieren. Anbieter von Communityplattformen verdienen an Mitgliedschaftsgebühren, durch den Verkauf von Werbefläche oder Kundenprofilen. Die Anbieter von Brandcommunitys bauen eine Beziehung zu ihren Kunden auf und pflegen diese über die Plattform (Weill & Vitale, 2001; Rappa, 2011; Casalo, Flavian & Guinaliu, 2008; Timmers, 2000). Beispiele für virtuelle Communitys sind Wikipedia, Facebook, YouTube, die Mini Community und viele mehr.

Collaboration Platform	Das Geschäftsmodell der kollaborativen Plattformen stellt unterstützende Werkzeuge der Informations- und Kommunikationstechnologie (IKT) für die Kollaboration zwischen Unternehmen (B2B) zur Verfügung. Diese Unterstützung kann durch Darstellungstechniken, anwendungstechnische Beratung oder durch Projektberatung (zum Beispiel für ein virtuelles Team) erfolgen. Gebühren werden für das Management der Plattform (Nutzungsgebühren oder Mitgliederbeiträge) erhoben oder für den Verkauf spezialisierter Tools (Design, Ablauforganisation, Dokumentenmanagement) (Rappa, 2011; Timmers, 2000).
Third Party Marketplace	Dieses B2B-Geschäftsmodell ist spezialisiert auf Outsourcing-Lösungen im Marketingbereich von E-Shops, übernimmt also das gesamte Web-Marketing von Drittunternehmen. Im Gegensatz zur E-Mall übernimmt der 3rd Party Marketplacer sämtliche Funktionen wie Angebot (Internet-Präsenz), Markenmanagement, Bestellung, Auftragsbearbeitung, Lieferung und Bezahlung. Beispiel eines Third Party Marketplace ist der Elektronikanbieter Best Buy. Umsätze generiert das Geschäftsmodell durch Aufnahmegebühren, Servicegebühren oder durch einen prozentualen Anteil an den Einnahmen (Timmers. 2000; Weill & Vitale, 2001).
Value-Chain Integrator	Value-Chain Integrators fokussieren auf die Integration mehrerer Prozessschritte der Wertschöpfungskette, um den Informationsfluss zwischen diesen Schritten zu optimieren. Die Prozessschritte werden so umgestaltet, dass ein höherer Kundennutzen und somit ein Mehrwert entsteht. Umsätze werden in diesem B2B-Geschäftsmodell über Beratungsgebühren oder Transaktionsgebühren generiert. Ein prominentes Beispiel ist die Website des amerikanischen Computer-Hardware-Herstellers Dell, auf welcher der Kunde seinen Computer nach seinen Wünschen zusammenstellen und zu sich nach Hause liefern lassen kann (Timmers, 2000; Tapscott, Ticoll & Lowy, 2000). Timmers (2000) prognostiziert eine Verschmelzung der Geschäftsmodelle Value-Chain Integrators und Value-Chain Service Providers.
Value-Chain Service Provider	Value-Chain Service Providers spezialisieren sich auf eine oder mehrere Stufen der Wertschöpfungskette, wie zum Beispiel die Zahlungsmöglichkeiten oder die Logistik, um in diesem Bereich Schlüsselkompetenzen aufzubauen. Unternehmen können einzelne Teile ihrer Wertschöpfungskette an Value-Chain Service Providers auslagern. Bei diesem B2C- und B2B-Geschäftsmodell ist es oft so, dass bisherige Schlüsselkompetenzen mit den Möglichkeiten des Internets ergänzt und verknüpft werden. Umsätze werden durch Gebühren oder einen prozentualen Anteil an den Einnahmen generiert (Tapscott et al., 2000; Timmers, 2000). Beispiele sind FedEx oder das World Net der Deutschen Post.
Information Broker / Trust Service	Viele neue Geschäftsideen entstehen im Bereich der Datensammlung und -aufbereitung. Sie nutzen die Unmengen von Daten im virtuellen Raum und filtern gezielt Informationen heraus. Oft sind Information Brokers als Startseite für Surfer gedacht; bekannte Portale im B2C-Bereich sind zum Beispiel Google oder Info-Scout, welche mit einer umfangreichen Suchfunktion ausgestattet sind (Timmers, 2000; Rappa, 2011). Information Brokers verdienen durch Abogebühren, Pay per Use oder durch den Verkauf von Werbung (Mahadevan, 2000). Eine spezielle Kategorie von Information Brokers sind Trust Services (Treuhanddienste), welche Zertifizierungen oder elektronische Unterschriften ausstellen. Diese Dienstleistung erfordert meistens eine staatliche Zertifizierung. Dafür werden Abonnementsgebühren oder Mitgliederbeiträge erhoben. Ein Beispiel eines B2B-Trust-Service-Anbieters ist die amerikanische Firma Verisign, welche Unternehmen auf ihre Identität und Sicherheit hin überprüft und Sicherheitszertifikate ausstellt (Timmers, 2000).

7.2 Qualitative Befragung der Anbieter

7.2.1 Leitfaden der Anbieter-Befragung

Zu Beginn der Interviews wurden den Gesprächspartnern Ausgangspunkt und Hintergrund des Projekts erläutert. Es wurde diskutiert, dass Online-Geschäftsmodelle häufig darauf beruhen, dass die Nutzer im Internet bereit sein müssen, dem Anbieter persönliche Daten bereitzustellen. Ohne persönliche Daten ist keine Transaktion im Internet möglich. Deshalb kann angenommen werden, dass Vertrauen ein kritischer Erfolgsfaktor für Anbieter von Online-Geschäftsmodellen ist. Nach dieser kurzen Diskussion wurde gefragt, ob das Gespräch für die Transkription aufgezeichnet werden darf und mit dem Fragebogen begonnen:

- Wie ist die Sicht des Unternehmens? Wie wird die Bedeutung des Kundenvertrauens eingeschätzt? Relevanz für das Geschäftsmodell?
- Warum Vertrauen Kunden Ihnen? Warum sind sie bereit, Ihnen ihre Daten anzuvertrauen?
- Hat die Unternehmenskommunikation einen Einfluss auf das Vertrauen der Kunden? Wie?
- Glauben Sie, dass die Kunden den Umgang mit ihren Daten reflektieren? Stellt der Datenschutz ein echtes Anliegen dar?
- Wie reagiert das Unternehmen darauf?
- Spielen „weiche“ Faktoren eine Rolle? Bspw. Layout/Design, Logos etc.
- Spielen Empfehlungen eine Rolle („Unterstützung/Empfehlung Dritter“): Stiftung Warentest, Testberichte…?
- Zeigen Bürger grosse Zurückhaltung, ihre Daten dem Staat anzuvertrauen? Sind Privatunternehmen hier in einem Vorteil? Warum?

7.2.2 Übersicht der geführten Interviews mit Anbietern von Online-Geschäftsmodellen

Nr.	Name	Geschäftsmodell	Gründungs-jahr	Rechtsform	Börsen-notiert	Umsatz 2008 (Mio. EUR)	Mitarbeiter	Interviewpartner	Interview Datum
A1	Google	Information Brokers	1998	AG	Ja	15'039	19'665	Legal Counsel	16.04.2009
A2	Geschenke	E-Shop / E-Mall	2007	GmbH	Nein	3	35	CEO	19.03.2009
A3	Gamesload**	E-Shop / E-Mall	2005	AG	Ja	61'700	260'000	Senior Manager	06.04.2009
A4	eBay	E-Auction	1995	AG	Ja	5'893	16'000	Manager Government Relations	05.03.2009
A5	DAB	E-Shop / E-Mall	1994	AG	Ja	137	693	Head of Corporate Communications	20.03.2009
A6	Cortal Consors	E-Shop / E-Mall	1994	AG	Nein	200*	1'500	Head of Corporate Communications	19.02.2009
A7	Buch	E-Shop / E-Mall	1998	AG	Ja	70	105	Head of Corporate Communications	04.03.2009
A8	Xing	Virtual Communitys	2003	AG	Ja	35	239	Head of Corporate Communications	23.03.2009
A9	Wunderloop	Information Brokers	1999	GmbH	Nein	n/a	55	CEO	26.03.2009
A10	Paypal	Value-Chain Service Provider	1998	GmbH	Nein	n/a	2'000	Sr. Manager Corporate Communications	09.03.2009
A11	Mitfahrzentrale	Collaboration Platforms	1998	GmbH	Nein	n/a	15	Head of Corporate Communications	20.04.2009
A12	Parship	Virtual Communitys	2000	GmbH	Nein	46*	190	Marketing Manager & Country Manager	12.03.2009
A13	Postbank	E-Shop / E-Mall	1989	AG	Ja	9'930	21'130	Head of Online Communication	19.03.2009
A14	Atizo	Collaboration Platforms	2008	GmbH	Nein	n/a	9	CEO	01.09.2009
A15	Doodle	Collaboration Platforms	2003	AG	Ja	n/a	9	Head of Corporate Communications	04.08.2009
A16	Guenstiger	Information Brokers	1999	GmbH	Nein	n/a	n/a	Press Spokesman	22.09.2009
A17	Auxion	E-Auction	1999	GmbH	Nein	n/a	n/a	Customer Consultant	17.09.2009
A18	Wordpress	Collaboration Platforms	2004	GmbH	Nein	n/a	40	Designer & Programmer	13.10.2009
A19	Experteer	Information Brokers	2005	GmbH	Nein	n/a	n/a	CEO	28.09.2009
A20	Deutsche Post	Value-Chain Service Provider	1995	AG	Ja	54'190	456'716	Vice President	26.10.2009
A21	Unister GmbH	Virtual Communitys	2002	GmbH	Nein	n/a	500	Head of Corporate Communications	01.09.2009

*Daten von 2007 **Daten der Muttergesellschaft

7.3 Qualitative Befragung der Nutzer

7.3.1 Leitfaden der Nutzer-Befragung

- Geschlecht: m/w
- Alter:
- Beruf:

- Arbeiten Sie beruflich mit dem Internet?
- Nutzen Sie das Internet privat?
- Wie oft nutzen Sie das Internet (jeden Tag, mehrmals pro Woche, weniger als einmal pro Woche)?

- Vertrauen Sie dem Medium Internet? Wieso?
- Welchem Internet-Anbieter vertrauen Sie? Wieso?
- Auf was achten Sie bei einem Anbieter?
- Nutzen Sie bewusst einen Anbieter nicht, weil Sie ihm nicht vertrauen?

- Welches sind für Sie Faktoren, welche das Vertrauen aufbaut/fördert (Online- & Offline-Welt)?
- Welches sind für Sie Faktoren, welche das Vertrauen zerstören (Online- & Offline-Welt)?

- Nutzen Sie Facebook / Online-Banking / Parship? Wieso? Wieso nicht?
- Vertrauen Sie Ihrer Bank (…) in Bezug auf Datensicherheit?

- Nutzen Sie Meinungsforen oder soziale Netzwerke für Ihre Informationssuche?
- Schreiben Sie selbst Meinungen oder Produktgutachten in Meinungsforen oder sozialen Netzwerken?

- Wann sind Sie bereit, einem Unternehmen persönliche Daten anzuvertrauen (Geburtsdatum, Bankdaten, sexuelle Präferenzen ...)?
- Haben Sie Bedenken bezüglich Privatheit Ihrer Daten? Haben Sie Angst um Ihre Daten? Aggregation der Daten?
- Ist Ihnen Datenschutz ein Anliegen? Haben Sie sich schon Gedanken darüber gemacht?
- Fühlen Sie sich durch ein Login mit Passwort sicherer?
- Achten Sie auf Gütesiegel wie zum Beispiel von Stiftung Warentest / Testberichte / Medienberichte oder aber Beurteilungen von anderen Nutzern?

- Vertrauen Sie eher Privatunternehmen oder vertrauen Sie eher dem Staat im Internet?

7.3.2 Übersicht der geführten Interviews mit Nutzern von Online-Geschäftsmodellen

Nr.	Geschlecht	Alter	Beruf	Branche	Bildungsabschluss	Interview Datum
N1	w	26–35	wiss. Mitarbeiterin	Bildung	Diplom	23.02.2010
N2	m	26–35	wiss. Mitarbeiter	Bildung	M. A.	02.03.2010
N3	m	26–35	wiss. Mitarbeiter	Bildung	Diplom	03.03.2010
N4	w	36–45	wiss. Mitarbeiterin	Bildung	Doktorat	03.03.2010
N5	w	46–55	Marketing	Bildung	Doktorat	04.03.2010
N6	m	26–35	Schauspieler	Kultur	Diplom	04.03.2010
N7	w	26–35	Kaufmännische Angestellte	Elektroindustrie	Berufsschule	05.03.2010
N8	m	26–35	Ingenieur	Energie	Doktorat	05.03.2010
N9	m	26–35	Ingenieur	Energie	Diplom	05.03.2010
N10	m	46–55	Maschinenbau-Ing.	Kraftwerke	Diplomingenieur FH	05.03.2010
N11	w	26–35	wiss. Mitarbeiterin	Bildung	Magister	08.03.2010
N12	m	26–35	Ingenieur	Energie	Diplom	08.03.2010
N13	w	26–35	Studentin (auf Stellensuche)	---	M. A.	09.03.2010
N14	w	26–35	wiss. Mitarbeiterin	Bildung	Diplom	11.03.2010
N15	m	56–65	Arzt	Medizin	Doktorat	11.03.2010
N16	m	26–35	wiss. Mitarbeiter	Bildung	Diplom	15.03.2010
N17	w	26–35	Bankkauffrau	Bank	Mittlere Reife	16.03.2010
N18	w	26–35	wiss. Mitarbeiterin	Bildung	Diplom	16.03.2010
N19	w	26–35	wiss. Mitarbeiterin	Bildung	Diplom	16.03.2010
N20	w	56–65	Praxisassistentin	Medizin	Diplom	16.03.2010
N21	w	< 25	Studentin	in Ausbildung	Abitur	17.03.2010
N22	m	26–35	Ingenieur	Energie	Diplom	17.03.2010
N23	w	26–35	wiss. Mitarbeiterin	Bildung	Diplom	23.03.2010
N24	w	< 25	Studentin	Bildung	Diplom	24.03.2010
N25	w	26–35	Schulpsychologin	Psychologie	Doktorat	09.04.2010
N26	m	66 +	Rentner	Kaufmann	Berufsschule	15.04.2010
N27	w	26–35	Journalistin	Medien	Abitur	26.04.2010
N28	w	26–35	Assistenz	Medizin	Staatsexamen	27.04.2010
N29	w	26–35	Assistenz	Medizin	Staatsexamen	27.04.2010
N30	m	36–45	Abteilungsleiter	Wissenschaft	Doktorat	27.04.2010
N31	w	< 25	Schüler	in Ausbildung	Hauptschulabschluss	27.04.2010
N32	w	< 25	Schüler	in Ausbildung	Hauptschulabschluss	27.04.2010
N33	w	< 25	Schüler	in Ausbildung	Hauptschulabschluss	27.04.2010
N34	w	< 25	Schüler	in Ausbildung	Realschulabschluss	27.04.2010
N35	w	< 25	Schüler	in Ausbildung	Realschulabschluss	27.04.2010
N36	w	26–35	Sozialpädagogin	Institution	Erlebnispädagogin	27.04.2010
N37	m	< 25	Schüler	in Ausbildung	Realschulabschluss	27.04.2010
N38	m	< 25	Maschinenbauingenieur	in Ausbildung	Diplom	27.04.2010
N39	m	56–65	Freischaffend	Automobilindustrie	Abitur	27.04.2010
N40	w	< 25	Schüler	in Ausbildung	Hauptschulabschluss	27.04.2010
N41	w	< 25	Schüler	in Ausbildung	Hauptschulabschluss	27.04.2010
N42	w	< 25	Kellnerin	in Ausbildung	Abitur	27.04.2010
N43	m	< 25	Schüler	in Ausbildung	Hauptschulabschluss	27.04.2010

7.4 Quantitative Online-Umfrage

7.4.1 Fragebogen der Online-Umfrage

Anfang

Institute for Media and Communications Management
University of St.Gallen

Herzlich Willkommen!

Diese Umfrage wird durchgeführt durch die Universität St. Gallen (Schweiz). Unsere Studie soll herausfinden, wie im Internet das Vertrauen der Nutzer entsteht. Alle Anworten sind anonym und werden vertraulich behandelt.
Die Umfrage dauert ca. 10 Minuten.

Wir danken Ihnen sehr für Ihre Teilnahme!

Quoten

Zum Einstieg benötigen wir wenige statistische Angaben zu Ihrer Person.

Geschlecht:

Weiblich ○ **Männlich** ○

Alter:

Bitte auswählen
bis 15
16-25
26-45
46-65
66 +

Höchster Bildungsabschluss:

- ○ Noch in schulischer Ausbildung
- ○ Hauptschulabschluss
- ○ Realschulabschluss
- ○ Berufslehre
- ○ Abitur / Fachabitur
- ○ Fachhochschule / Studium
- ○ Sonstige

Erwerbstätigkeit:

- ○ Angestellt (Vollzeit / Teilzeit)
- ○ Selbstständig erwerbstätig
- ○ Arbeitssuchend
- ○ keine Angabe
- ○ in Ausbildung / Lehre
- ○ in Rente
- ○ Hausfrau / -mann

Branche:

- ○ Automobil / Luftfahrt / Schifffahrt
- ○ Bauwesen / Infrastruktur
- ○ Beratung / Recht
- ○ Energie / Umwelt / Recycling
- ○ Finanzen / Versicherung / Immobilien
- ○ Gesundheits- & Sozialwesen
- ○ Gross- und Einzelhandel
- ○ Informations- & Kommunikationstechnologien / Elektronische Geräte
- ○ Sonstiges
- ○ Kommunikation / Medien
- ○ Landwirtschaft / Bergbau
- ○ Maschinenbau
- ○ Medizin / Pharma / Chemie
- ○ Nahrungs- und Genussmittel
- ○ Öffentlicher Dienst
- ○ Tourismus / Gastgewerbe / Kultur / Sport
- ○ Transport / Logistik

Einstieg

Wie oft nutzen Sie das Internet?

- jeden Tag
- mehrmals pro Woche
- einmal pro Woche
- 1- bis 2-mal im Monat
- seltener

Seit wie vielen Jahren nutzen Sie das Internet?

Bitte auswählen
< 1 Jahr
seit 1 Jahr
seit 2 Jahren
seit 3 Jahren
seit 4 Jahren
seit 5 Jahren
seit 6 Jahren
seit 7 Jahren
seit 8 Jahren
> 8 Jahren

Wie nutzen Sie das Internet?

- ausschliesslich beruflich
- überwiegend beruflich
- sowohl beruflich als auch privat
- überwiegend privat
- ausschliesslich privat

Einstieg - 1

Wie oft nutzen Sie folgende Online-Dienste?

	jeden Tag	mehrmals pro Woche	einmal pro Woche	1- bis 2-mal im Monat	seltener	nie
eMail	○	○	○	○	○	○
Informationssuche (z.B. auf Google)	○	○	○	○	○	○
Online-Banking	○	○	○	○	○	○
Soziale Netzwerke/Online-Communities (z.B. Facebook / Xing)	○	○	○	○	○	○
Online-Shopping	○	○	○	○	○	○
Online-Zeitung	○	○	○	○	○	○
Online-TV/Radio	○	○	○	○	○	○
Online-Dating	○	○	○	○	○	○
Blogs	○	○	○	○	○	○
Twitter	○	○	○	○	○	○
Online-Games	○	○	○	○	○	○
Sonstige:	○	○	○	○	○	○

Einstieg - 2

Bitte beurteilen Sie die folgenden Aussagen:

	trifft zu	trifft eher zu	neutral	trifft eher nicht zu	trifft nicht zu
Ich habe keine Bedenken, Online-Transaktionen durchzuführen.	○	○	○	○	○
Manchmal fühle ich mich unsicher, wenn ich im Internet meinen Interessen nachgehe.	○	○	○	○	○
Online-Anbieter übervorteilen normalerweise ihre Kunden nicht.	○	○	○	○	○
Online-Anbieter behandeln ihre Kunden grundsätzlich anständig.	○	○	○	○	○
Es gibt genug Sicherheitsmechanismen im Internet, damit ich es bedenkenlos für meine persönlichen Interessen nutzen kann.	○	○	○	○	○
Ich vertraue darauf, dass mich rechtliche Rahmenbedingungen vor Problemen im Internet bewahren.	○	○	○	○	○
Ich vertraue darauf, dass mich technische Anwendungen vor Problemen im Internet bewahren (z.B. Verschlüsselungen).	○	○	○	○	○
Im Allgemeinen ist das Internet eine stabile und sichere Umgebung, um persönlichen Interessen nachzugehen.	○	○	○	○	○

Bitte beurteilen Sie die folgenden Aussagen:

	trifft zu	trifft eher zu	neutral	trifft eher nicht zu	trifft nicht zu
Im Allgemeinen habe ich Vertrauen zu anderen Menschen.	○	○	○	○	○
Ich verlasse mich meistens auf andere Menschen.	○	○	○	○	○
Im Grossen und Ganzen habe ich Vertrauen in die Menschheit.	○	○	○	○	○
Ich bin der Meinung, dass Menschen generell zuverlässig sind.	○	○	○	○	○
Im Allgemeinen vertraue ich anderen Menschen, ausser es gibt Gründe, dies nicht zu tun.	○	○	○	○	○

Einstieg - 3

Bitte beurteilen Sie die folgenden Aussagen:

	trifft zu	trifft eher zu	neutral	trifft eher nicht zu	trifft nicht zu
Ich kann mir relevante Informationen im Internet beschaffen.	○	○	○	○	○
Ich kann abschätzen, welche Informationen im Internet zuverlässig sind.	○	○	○	○	○
Ich vertraue meiner Fähigkeit, die Qualität einer Website einzuschätzen.	○	○	○	○	○
Ich bin in der Lage, ein Profil in einem Sozialen Netzwerk anzulegen.	○	○	○	○	○
Ich bin in der Lage, ein Video im Internet zu publizieren (z.B. auf Youtube).	○	○	○	○	○
Ich bin in der Lage, Informationen auf einem Blog oder bei Twitter zu veröffentlichen.	○	○	○	○	○
Ich kann meine Gedanken und Ideen im Internet mitteilen.	○	○	○	○	○
Ich bin in der Lage, einen Beitrag auf Wikipedia zu erstellen oder zu ergänzen.	○	○	○	○	○
Ich interessiere mich für neue Entwicklungen im Internet.	○	○	○	○	○
Ich probiere gerne neue Online-Plattformen und Applikationen aus.	○	○	○	○	○

2. Teil Vertrauensfaktoren

Denken Sie an den letzten Online-Anbieter, bei dem Sie sich als Nutzer registriert haben, wobei die Anmeldung die Eingabe einiger persönlicher Daten erforderte (z.B. für das Anlegen eines persönlichen Nutzer-Profils).

Um welche Art von Online-Angebot handelte es sich dabei? Bitte wählen Sie aus der folgenden Liste:

- ○ Online-Shopping (z.B. Amazon, eBay, Lufthansa)
- ○ Online-Banking (z.B. Comdirect, Postbank, PayPal)
- ○ Soziale Netzwerke / Online-Community (z.B. Facebook, Xing, Parship)
- ○ Online-Information (z.B. Google, Zeitungen, Blogs, eMail, YouTube)

Bitte nennen Sie den Anbieter, an den Sie denken:

Wie schätzen Sie den von Ihnen ausgewählten Anbieter ein?

	trifft zu	trifft eher zu	neutral	trifft eher nicht zu	trifft nicht zu
Wohlwollend	○	○	○	○	○
Kompetent	○	○	○	○	○
Ehrlich	○	○	○	○	○
Zuverlässig	○	○	○	○	○
Vertrauenswürdig	○	○	○	○	○
Sympathisch	○	○	○	○	○

Bitte beurteilen Sie die folgenden Aussagen:

	trifft zu	trifft eher zu	neutral	trifft eher nicht zu	trifft nicht zu
Ich werde die Seite des gewählten Anbieters wahrscheinlich wieder besuchen.	○	○	○	○	○
Ich werde die Dienste des gewählten Anbieters in den nächsten 3 Monaten erneut in Anspruch nehmen.	○	○	○	○	○
Ich würde die Seite des gewählten Anbieters anderen Personen weiterempfehlen.	○	○	○	○	○
Ich finde es unproblematisch, dem gewählten Anbieter persönliche Daten zu überlassen.	○	○	○	○	○
Ich glaube, dass ich mich auf die Angebotsqualität des gewählten Anbieters verlassen kann.	○	○	○	○	○

2. Teil - 1

Wie stark haben Sie auf folgende Eigenschaften geachtet, als Sie sich beim ausgewählten Anbieter angemeldet haben? Bitte beziehen Sie sich dabei auf den oben genannten Anbieter.

	stark beachtet	beachtet	neutral	wenig beachtet	nicht beachtet
Es ist gut erkennbar, welche Verpflichtungen ich eingehe (z.B. Kosten).	○	○	○	○	○
Die Allgemeinen Geschäftsbedingungen sind leicht zu finden.	○	○	○	○	○
Der Anbieter verfügt über strikte Datenschutzrichtlinien.	○	○	○	○	○
Der Anbieter bietet viele Informationen über das eigene Unternehmen.	○	○	○	○	○
Der Anbieter zeigt nachvollziehbar auf, wie er meine Daten verwendet.	○	○	○	○	○
Es ist gut erkennbar, welche Rechte ich dem Anbieter gegenüber habe (z.B. Garantien, Rückgaberecht).	○	○	○	○	○
Der Anbieter fragt nur Daten ab, die er benötigt, um seinen Dienst betreiben zu können.	○	○	○	○	○
Der Umfang der abgefragten Daten steht in einem passenden Verhältnis zum Nutzen, den mir der Dienst bietet.	○	○	○	○	○
Die Allgemeinen Geschäftsbedingungen sind einfach zu verstehen.	○	○	○	○	○
Der Anbieter bietet mir genau was ich suche.	○	○	○	○	○
Die Datenschutzbestimmungen sind leicht verständlich.	○	○	○	○	○
Ich empfinde die abgefragten Daten nicht als heikel oder zu persönlich.	○	○	○	○	○
Der Anbieter erklärt mir, warum er welche Daten von mir benötigt.	○	○	○	○	○
Die Datenschutzbestimmungen sind leicht zu finden.	○	○	○	○	○

2. Teil - 2

Wie stark haben Sie auf folgende Eigenschaften geachtet, als Sie sich beim ausgewählten Anbieter angemeldet haben? Bitte beziehen Sie sich dabei auf den oben genannten Anbieter.

	stark beachtet	beachtet	neutral	wenig beachtet	nicht beachtet
Links sind gut kenntlich gemacht.	○	○	○	○	○
Der Anbieter hat bereits viele Kunden bzw. Nutzer.	○	○	○	○	○
Es handelt sich um einen bekannten Anbieter.	○	○	○	○	○
Der Anbieter existiert schon eine Weile.	○	○	○	○	○
Die Nutzung des Dienstes funktioniert genau so, wie ich das von ähnlichen Diensten schon kenne.	○	○	○	○	○
Die Seite des Anbieters ist einfach und übersichtlich gestaltet.	○	○	○	○	○
Der Anbieter ist führend in seinem Bereich.	○	○	○	○	○
Ich fühle mich auf der Seite wohl.	○	○	○	○	○
Das Design des Anbieters wirkt seriös und professionell.	○	○	○	○	○

2. Teil - 3

Wie stark haben Sie auf folgende Eigenschaften geachtet, als Sie sich beim ausgewählten Anbieter angemeldet haben? Bitte beziehen Sie sich dabei auf den oben genannten Anbieter.

	stark beachtet	beachtet	neutral	wenig beachtet	nicht beachtet
Es kommt nicht zu technischen Fehlern.	○	○	○	○	○
Ich kenne das Unternehmen auch ausserhalb des Internets.	○	○	○	○	○
Der Anbieter stellt unterschiedliche Zahlungsmethoden zur Verfügung.	○	○	○	○	○
Die Seite lädt schnell.	○	○	○	○	○
Der Anbieter besitzt Filialen, die ich aufsuchen kann.	○	○	○	○	○
Informationen über den Anbieter sind einfach zu finden (z.B. Grösse, Mitarbeiter, Geschichte).	○	○	○	○	○
Der Kundendienst ist einfach erreichbar.	○	○	○	○	○
Der Anbieter reagiert schnell auf meine Fragen/Bestellungen.	○	○	○	○	○
Ich kann erkennen, dass der Anbieter seine Systeme gut vor fremden Eingriffen schützt (z.B. durch Verschlüsselung).	○	○	○	○	○
Die Seite des Anbieters stürzt nicht ab.	○	○	○	○	○
Die Kontaktdaten des Anbieters sind einfach zu finden (z.B. Adresse, Telefonnummer).	○	○	○	○	○
Die Büros des Anbieters werden auf einem Foto gezeigt.	○	○	○	○	○
Der Kundenservice des Anbieters ist freundlich.	○	○	○	○	○
Der Anbieter stellt unterschiedliche Möglichkeiten zur Kontaktaufnahme zur Verfügung (Telefonnummer, eMail, Adresse).	○	○	○	○	○

2. Teil - 4

Wie stark haben Sie auf folgende Eigenschaften geachtet, als Sie sich beim ausgewählten Anbieter angemeldet haben? Bitte beziehen Sie sich dabei auf den oben genannten Anbieter.

	stark beachtet	beachtet	neutral	wenig beachtet	nicht beachtet
Der Anbieter wurde mir von einem Bekannten empfohlen.	○	○	○	○	○
Der Anbieter fragt mich um meine Zustimmung, bevor er meine Daten an Dritte weitergibt.	○	○	○	○	○
Der Anbieter wird von anderen Nutzern positiv eingeschätzt (Ratings).	○	○	○	○	○
Der Anbieter wurde von einer unabhängigen Organisation getestet und mit einem Gütesiegel ausgezeichnet (z.B. Stiftung Warentest).	○	○	○	○	○
Der Anbieter verzichtet ausdrücklich auf die Weitergabe meiner Daten an Dritte.	○	○	○	○	○
Der Anbieter informiert mich, wenn er meine Daten an Dritte weitergibt.	○	○	○	○	○
Ich habe keine negativen Berichte über den Anbieter in der Presse gelesen.	○	○	○	○	○
Der Anbieter teilt mir mit, auf welche Art er meine Daten auswertet/analysiert.	○	○	○	○	○
Der Anbieter wird bei Suchmaschinen (z.B. Google) als eine der ersten Seiten aufgelistet.	○	○	○	○	○
Der Anbieter ermöglicht mir, selbst auszuwählen, an wen meine Daten weitergegeben werden.	○	○	○	○	○
Die Angabe von Daten über das notwendige Minimum hinaus ist freiwillig.	○	○	○	○	○
Ich weiss, welche meiner Daten der Anbieter gesammelt/gespeichert hat.	○	○	○	○	○
Der Anbieter wurde für seine Qualität mit Preisen ausgezeichnet.	○	○	○	○	○

3. Teil: Persönliche Daten

Zum Abschluss: Welche der folgenden Daten mussten Sie angeben, als Sie sich beim genannten Anbieter angemeldet haben?

- ☐ Vor- und Nachname
- ☐ User-Name / Pseudonym
- ☐ Geschlecht
- ☐ Strasse & Hausnummer
- ☐ Postleitzahl / Ort
- ☐ Telefonnummer
- ☐ eMail
- ☐ Geburtsdatum
- ☐ Geburtsjahr/Alter
- ☐ Bildungsabschluss
- ☐ Beruf
- ☐ Branche
- ☐ Zivilstand
- ☐ Sexuelle Orientierung
- ☐ Einkommensdaten
- ☐ Bankverbindung (Kontodaten)
- ☐ Kreditkarten
- ☐ ID / Passnummer
- ☐ Kontaktdaten von Freunden/Bekannten
- ☐ Fotos

Endseite

Herzlichen Dank für Ihre Teilnahme!

Zurück zu Panelbiz

7.4.2 Zusammensetzung der Stichprobe der Online-Umfrage (n = 1'549)

		Prozentsatz
Geschlecht	Weiblich	49.0
(V_135)	Männlich	48.0
	keine Angabe	3.0
Alter	bis 15	10.1
(V_136)	16–25	11.8
	26–45	26.2
	46–65	26.4
	66 +	19.6
	keine Angabe	5.8
Höchster Bildungsabschluss	Hauptschulabschluss	6.2
(V_139)	Realschulabschluss	16.8
	Berufsschule	20.1
	Abitur / Fachabitur	17.6
	Fachhochschule / Studium	24.9
	noch in schulischer Ausbildung	12.5
	Sonstige	1.5
	keine Angabe	0.4
Erwerbstätigkeit	Angestellt (Vollzeit / Teilzeit)	38.1
(V_137)	Selbständig erwerbstätig	9.4
	Arbeitssuchend	3.6
	in Ausbildung / Lehre	12.0
	in Rente	24.1
	Hausfrau / Hausmann	4.3
	keine Angabe	8.5
Internetnutzung	jeden Tag	91.9
(V_1)	mehrmals pro Woche	7.3
	weniger als einmal pro Woche	0.0
	keine Angabe	0.8
Jahre der Internetnutzung	< 1 Jahren	0.2
(V_2)	seit 1 Jahren	0.5
	seit 2 Jahren	1.4
	seit 3 Jahren	4.7
	seit 4 Jahren	5.6
	seit 5 Jahren	10.5
	seit 6 Jahren	7.5
	seit 7 Jahren	5.4
	seit 8 Jahren	7.7
	> 8 Jahren	54.9
	keine Angabe	1.6
Art der Internetnutzung	ausschliesslich beruflich	0.2
(V_3)	überwiegend beruflich	1.2
	sowohl beruflich als auch privat	47.7
	überwiegend privat	23.7
	ausschliesslich privat	26.7
	keine Angabe	0.5

7.4.3 Finale Item-Liste der Vertrauensfaktoren

Ex_V_Name	**Reziprozität**
V_67	Der Anbieter fragt nur Daten ab, die er benötigt, um seinen Dienst betreiben zu können.
V_68	Der Anbieter erklärt mir, warum er welche Daten von mir benötigt.
V_69	Der Umfang der abgefragten Daten steht in einem passenden Verhältnis zum Nutzen, den mir der Dienst bietet.
V_70	Ich empfinde die abgefragten Seiten nicht als heikel oder zu persönlich.
V_71	Der Anbieter zeigt nachvollziehbar auf, wie er meine Daten verwendet.
V_72	Die Datenschutzbestimmungen sind leicht zu finden.
V_73	Die Datenschutzbestimmungen sind leicht verständlich.
V_74	Der Anbieter verfügt über strikte Datenschutzrichtlinien.
V_75	Die allgemeinen Geschäftsbedingungen sind leicht zu finden.
V_76	Die allgemeinen Geschäftsbedingungen sind einfach zu verstehen.
V_77	Es ist gut erkennbar, welche Verpflichtungen ich eingehe (z. B. Kosten).
V_78	Es ist gut erkennbar, welche Rechte ich dem Anbieter gegenüber habe (z. B. Garantien, Rückgaberecht).
V_79	Der Anbieter bietet viele Informationen über das eigene Unternehmen.

Ex_V_Name	**Marke und Design**
V_94	Es handelt sich um einen bekannten Anbieter.
V_95	Der Anbieter ist führend in seinem Bereich.
V_96	Der Anbieter existiert schon eine Weile.
V_97	Der Anbieter hat bereits viele Kunden bzw. Nutzer.
V_98	Das Design des Anbieters wirkt seriös und professionell.
V_100	Die Seite des Anbieters ist einfach und übersichtlich gestaltet.
V_1001	Links sind gut kenntlich gemacht.
V_102	Die Nutzung des Dienstes funktioniert genau so, wie ich das von ähnlichen Diensten schon kenne.
V_103	Ich fühle mich auf der Seite wohl.

Ex_V_Name	**Kundenservice**
V_109	Die Kontaktdaten des Anbieters sind einfach zu finden (z. B. Adresse, Telefonnummer).
V_114	Der Kundendienst ist einfach erreichbar.
V_115	Der Anbieter reagiert schnell auf meine Fragen/Bestellungen.
V_116	Der Anbieter stellt unterschiedliche Zahlungsmethoden zur Verfügung.
V_179	Der Kundenservice des Anbieters ist freundlich.
V_180	Der Anbieter stellt unterschiedliche Möglichkeiten zur Kontaktaufnahme zur Verfügung (Telefonnummer, E-Mail, Adresse).

Ex_V_Name	Nutzerkontrolle
V_117	Die Angabe von Daten über das notwendige Minimum hinaus ist freiwillig.
V_118	Ich weiss, welche meiner Daten der Anbieter gesammelt/gespeichert hat.
V_119	Der Anbieter informiert mich, wenn er meine Daten an Dritte weitergibt.
V_120	Der Anbieter fragt mich um meine Zustimmung, bevor er meine Daten an Dritte weitergibt.
V_121	Der Anbieter verzichtet ausdrücklich auf die Weitergabe meiner Daten an Dritte.
V_122	Der Anbieter ermöglicht mir, selbst auszuwählen, an wen meine Daten weitergegeben werden.
V_123	Der Anbieter teilt mir mit, auf welche Art er meine Daten auswertet/analysiert.

Ex_V_Name	Realweltbezug
V_104	Der Anbieter besitzt Filialen, die ich aufsuchen kann.
V_105	Ich kenne das Unternehmen auch ausserhalb des Internets.
V_106	Informationen über den Anbieter sind einfach zu finden (z. B. Grösse, Mitarbeiter, Geschichte).
V_108	Die Büros des Anbieters werden auf einem Foto gezeigt.

Ex_V_Name	Technik
VV_110	Es kommt nicht zu technischen Fehlern.
V_111	Die Seite des Anbieters stürzt nicht ab.
V_112	Die Seite lädt schnell.
V_113	Ich kann erkennen, dass der Anbieter seine Systeme gut vor fremden Eingriffen schützt (z. B. durch Verschlüsselung).
V_66	Der Anbieter bietet mir genau was ich suche.

Ex_V_Name	Empfehlungen
V_126	Der Anbieter wird bei Suchmaschinen (z. B. Google) als eine der ersten Seiten aufgelistet.
V_125	Der Anbieter wurde mir von einem Bekannten empfohlen.
V_128	Der Anbieter wurde für seine Qualität mit Preisen ausgezeichnet.
V_129	Ich habe keine negativen Berichte über den Anbieter in der Presse gelesen.
V_130	Der Anbieter wird von anderen Nutzern positiv eingeschätzt (Ratings).
V_127	Der Anbieter wurde von einer unabhängigen Organisation getestet und mit einem Gütesiegel ausgezeichnet (z. B. Stiftung Warentest).

7.4.4 Faktorladungsmatrix für die Auswertung der Vertrauensfaktoren

Rotated Component Matrix[a]

	1	2	3	4	5	6
V_73 Die Datenschutzbestimmungen sind leicht verständlich.	.794					
V_76 Die allgemeinen Geschäftsbedingungen sind einfach zu verstehen.	.780					
V_72 Die Datenschutzbestimmungen sind leicht zu finden.	.766					
V_75 Die allgemeinen Geschäftsbedingungen sind leicht zu finden.	.746					
V_74 Der Anbieter verfügt über strikte Datenschutz-richtlinien.	.716					
V_78 Es ist gut erkennbar, welche Rechte ich dem Anbieter gegenüber habe (z. B. Garantien, Rückga-berecht).	.680					
V_68 Der Anbieter erklärt mir, warum er welche Daten von mir benötigt.	.677					
V_71 Der Anbieter zeigt nachvollziehbar auf, wie er meine Daten verwendet.	.667					
V_79 Der Anbieter bietet viele Informationen über das eigene Unternehmen.	.620					
V_67 Der Anbieter fragt nur Daten ab, die er benö-tigt, um seinen Dienst betreiben zu können.	.608					
V_77 Es ist gut erkennbar, welche Verpflichtungen ich eingehe (z. B. Kosten).	.544					
V_94 Es handelt sich um einen bekannten Anbieter.		.807				
V_97 Der Anbieter hat bereits viele Kunden bzw. Nutzer.		.791				
V_96 Der Anbieter existiert schon eine Weile.		.781				
V_100 Die Seite des Anbieters ist einfach und über-sichtlich gestaltet.		.755				
V_95 Der Anbieter ist führend in seinem Bereich.		.746				
V_98 Das Design des Anbieters wirkt seriös und professionell.		.721				
V_102 Die Nutzung des Dienstes funktioniert genau so, wie ich das von ähnlichen Diensten schon kenne.		.711				
V_103 Ich fühle mich auf der Seite wohl.		.723				
V_101 Links sind gut kenntlich gemacht.		.699				
V_180 Der Anbieter stellt unterschiedliche Möglich-keiten zur Kontaktaufnahme zur Verfügung (Tele-fonnummer, E-Mail, Adresse).				.716		
V_179 Der Kundenservice des Anbieters ist freund-lich.				.700		
V_114 Der Kundendienst ist einfach erreichbar.				.698		
V_115 Der Anbieter reagiert schnell auf meine Fra-gen/Bestellungen.				.697		
V_109 Die Kontaktdaten des Anbieters sind einfach zu finden (z. B. Adresse, Telefonnummer).				.698		
V_116 Der Anbieter stellt unterschiedliche Zah-lungsmethoden zur Verfügung.				.693		

V_119 Der Anbieter informiert mich, wenn er meine Daten an Dritte weitergibt.	.742		
V_120 Der Anbieter fragt mich um meine Zustimmung, bevor er meine Daten an Dritte weitergibt.	.728		
V_122 Der Anbieter ermöglicht mir, selbst auszuwählen, an wen meine Daten weitergegeben werden.	.694		
V_117 Die Angabe von Daten über das notwendige Minimum hinaus ist freiwillig.	.672		
V_123 Der Anbieter teilt mir mit, auf welche Art er meine Daten auswertet/analysiert.	.678		
V_121 Der Anbieter verzichtet ausdrücklich auf die Weitergabe meiner Daten an Dritte.	.656		
V_118 Ich weiss, welche meiner Daten der Anbieter gesammelt/gespeichert hat.	.630		
V_126 Der Anbieter wird bei Suchmaschinen (z. B. Google) als eine der ersten Seiten aufgelistet.			.639
V_128 Der Anbieter wurde für seine Qualität mit Preisen ausgezeichnet.			.541
V_127 Der Anbieter wurde von einer unabhängigen Organisation getestet und mit einem Gütesiegel ausgezeichnet (z. B. Stiftung Warentest).			.533
V_104 Der Anbieter besitzt Filialen, die ich aufsuchen kann.		.803	
V_105 Ich kenne das Unternehmen auch ausserhalb des Internets.		.792	
V_108 Die Büros des Anbieters werden auf einem Foto gezeigt.		.705	
V_106 Informationen über den Anbieter sind einfach zu finden (z. B. Grösse, Mitarbeiter, Geschichte).		.529	

7.4.5 Rotierte Faktorladungen und Extraktionswerte für die Auswertung der Vertrauensfaktoren

Reziprozität

Faktor 1	F-Ladung	Extraktion
V_73 Die Datenschutzbestimmungen sind leicht verständlich.	0.794	0.745
V_76 Die allgemeinen Geschäftsbedingungen sind einfach zu verstehen.	0.780	0.700
V_72 Die Datenschutzbestimmungen sind leicht zu finden.	0.766	0.704
V_75 Die allgemeinen Geschäftsbedingungen sind leicht zu finden.	0.746	0.675
V_74 Der Anbieter verfügt über strikte Datenschutzrichtlinien.	0.716	0.674
V_78 Es ist gut erkennbar, welche Rechte ich dem Anbieter gegenüber habe (z. B. Garantien, Rückgaberecht).	0.680	0.658
V_68 Der Anbieter erklärt mir, warum er welche Daten von mir benötigt.	0.677	0.601
V_71 Der Anbieter zeigt nachvollziehbar auf, wie er meine Daten verwendet.	0.667	0.603
V_79 Der Anbieter bietet viele Informationen über das eigene Unternehmen.	0.620	0.606
V_67 Der Anbieter fragt nur Daten ab, die er benötigt, um seinen Dienst betreiben zu können.	0.608	0.593
V_77 Es ist gut erkennbar, welche Verpflichtungen ich eingehe (z. B. Kosten).	0.544	0.551
		Cronbachs Alpha = 0.934

Marke und Design

Faktor 2	F-Ladung	Extraktion
V_94 Es handelt sich um einen bekannten Anbieter.	0.807	0.690
V_97 Der Anbieter hat bereits viele Kunden bzw. Nutzer.	0.791	0.690
V_96 Der Anbieter existiert schon eine Weile.	0.781	0.671
V_100 Die Seite des Anbieters ist einfach und übersichtlich gestaltet.	0.755	0.688
V_95 Der Anbieter ist führend in seinem Bereich.	0.746	0.639
V_98 Das Design des Anbieters wirkt seriös und professionell.	0.721	0.620
V_102 Die Nutzung des Dienstes funktioniert genau so, wie ich das von ähnlichen Diensten schon kenne.	0.711	0.604
V_103 Ich fühle mich auf der Seite wohl.	0.723	0.622
V_101 Links sind gut kenntlich gemacht.	0.699	0.597
		Cronbachs Alpha = 0.926

Nutzerkontrolle

Faktor 3	F-Ladung	Extraktion
V_119 Der Anbieter informiert mich, wenn er meine Daten an Dritte weitergibt.	0.742	0.693
V_120 Der Anbieter fragt mich um meine Zustimmung, bevor er meine Daten an Dritte weitergibt.	0.728	0.650
V_122 Der Anbieter ermöglicht mir, selbst auszuwählen, an wen meine Daten weitergegeben werden.	0.694	0.623
V_117 Die Angabe von Daten über das notwendige Minimum hinaus ist freiwillig.	0.672	0.575
V_123 Der Anbieter teilt mir mit, auf welche Art er meine Daten auswertet/analysiert.	0.678	0.652
V_121 Der Anbieter verzichtet ausdrücklich auf die Weitergabe meiner Daten an Dritte.	0.656	0.601
V_118 Ich weiss, welche meiner Daten der Anbieter gesammelt/gespeichert hat.	0.630	0.584
		Cronbachs Alpha = 0.893

Kundenservice

Faktor 4	F-Ladung	Extraktion
V_180 Der Anbieter stellt unterschiedliche Möglichkeiten zur Kontaktaufnahme zur Verfügung (Telefonnummer, E-Mail, Adresse).	0.716	0.701
V_179 Der Kundenservice des Anbieters ist freundlich.	0.700	0.700
V_114 Der Kundendienst ist einfach erreichbar.	0.698	0.701
V_115 Der Anbieter reagiert schnell auf meine Fragen/Bestellungen.	0.697	0.646
V_109 Die Kontaktdaten des Anbieters sind einfach zu finden (z. B. Adresse, Telefonnummer).	0.698	0.699
V_116 Der Anbieter stellt unterschiedliche Zahlungsmethoden zur Verfügung.	0.693	0.578
	Cronbachs Alpha = 0.899	

Realweltbezug

Faktor 5	F-Ladung	Extraktion
V_104 Der Anbieter besitzt Filialen, die ich aufsuchen kann.	0.803	0.747
V_105 Ich kenne das Unternehmen auch ausserhalb des Internets.	0.792	0.735
V_108 Die Büros des Anbieters werden auf einem Foto gezeigt.	0.705	0.671
V_106 Informationen über den Anbieter sind einfach zu finden (z. B. Grösse, Mitarbeiter, Geschichte).	0.529	0.590
	Cronbachs Alpha = 0.826	

Empfehlungen

Faktor 6	F-Ladung	Extraktion
V_126 Der Anbieter wird bei Suchmaschinen (z. B. Google) als eine der ersten Seiten aufgelistet.	0.639	0.582
V_128 Der Anbieter wurde für seine Qualität mit Preisen ausgezeichnet.	0.541	0.635
V_127 Der Anbieter wurde von einer unabhängigen Organisation getestet und mit einem Gütesiegel ausgezeichnet (z. B. Stiftung Warentest).	0.533	0.633
	Cronbachs Alpha = 0.743	

Ausgeschlossene Items[57]

V_66 Der Anbieter bietet mir genau was ich suche.
V_69 Der Umfang der abgefragten Daten steht in einem passenden Verhältnis zum Nutzen, den mir der Dienst bietet.
V_70 Ich empfinde die abgefragten Seiten nicht als heikel oder zu persönlich.
V_110 Es kommt nicht zu technischen Fehlern.
V_111 Die Seite des Anbieters stürzt nicht ab.
V_112 Die Seite lädt schnell.
V_113 Ich kann erkennen, dass der Anbieter seine Systeme gut vor fremden Eingriffen schützt (z. B. durch Verschlüsselung).
V_125 Der Anbieter wurde mir von einem Bekannten empfohlen.
V_129 Ich habe keine negativen Berichte über den Anbieter in der Presse gelesen.
V_130 Der Anbieter wird von anderen Nutzern positiv eingeschätzt (Ratings).

[57] Da bei diesen zehn Items entweder die Extraktion oder die Faktorladung zu gering war, wurden sie aus der Analyse ausgeschlossen.

7.4.6 Faktorladungsmatrix für die Auswertung des Vertrauensmasses

Rotated Component Matrix

	1	2	3	4
V_20 Online-Anbieter behandeln ihre Kunden grundsätzlich anständig.			.613	
V_21 Es gibt genug Sicherheitsmechanismen im Internet, damit ich es bedenkenlos für meine persönlichen Interessen nutzen kann.			.809	
V_22 Ich vertraue darauf, dass mich rechtliche Rahmenbedingungen vor Problemen im Internet bewahren.			.814	
V_23 Ich vertraue darauf, dass mich technische Anwendungen vor Problemen im Internet bewahren (z. B. Verschlüsselungen).			.798	
V_24 Im Allgemeinen ist das Internet eine stabile und sichere Umgebung, um persönlichen Interessen nachzugehen.			.765	
V_25 Im Allgemeinen habe ich Vertrauen zu anderen Menschen.		.820		
V_26 Ich verlasse mich meistens auf andere Menschen.		.741		
V_27 Im Grossen und Ganzen habe ich Vertrauen in die Menschheit.		.815		
V_28 Ich bin der Meinung, dass Menschen generell zuverlässig sind.		.759		
V_29 Im Allgemeinen vertraue ich anderen Menschen, ausser es gibt Gründe, dies nicht zu tun.		.777		
V_56 Wohlwollend	.812			
V_57 Kompetent	.834			
V_58 Ehrlich	.901			
V_59 Zuverlässig	.874			
V_60 Vertrauenswürdig	.886			
V_176 Sympathisch	.782			
V_61 Ich werde die Seite des gewählten Anbieters wahrscheinlich wieder besuchen.				.837
V_62 Ich werde die Dienste des gewählten Anbieters in den nächsten drei Monaten erneut in Anspruch nehmen.				.884
V_63 Ich würde die Seite des gewählten Anbieters anderen Personen weiterempfehlen.				.676
V_64 Ich finde es unproblematisch, dem gewählten Anbieter persönliche Daten zu überlassen.	.648			
V_65 Ich glaube, dass ich mich auf die Angebotsqualität des gewählten Anbieters verlassen kann.	.695			

7.4.7 Rotierte Faktorladungen und Extraktionswerte für die Auswertung des Vertrauensmasses[58]

Vertrauen in den Anbieter

Faktor 1	F-Ladung	Extraktion
V_56 Wohlwollend	.812	.693
V_57 Kompetent	.834	.761
V_58 Ehrlich	.901	.842
V_59 Zuverlässig	.874	.796
V_60 Vertrauenswürdig	.886	.815
V_176 Sympathisch	.782	.669
V_64 Ich finde es unproblematisch, dem gewählten Anbieter persönliche Daten zu überlassen.	.648	.532
V_65 Ich glaube, dass ich mich auf die Angebotsqualität des gewählten Anbieters verlassen kann.	.695	.661
		Cronbachs Alpha = 0.938

Vertrauensneigung (Disposition to Trust)

Faktor 2	F-Ladung	Extraktion
V_25 Im Allgemeinen habe ich Vertrauen zu anderen Menschen.	.820	.700
V_26 Ich verlasse mich meistens auf andere Menschen.	.741	.563
V_27 Im Grossen und Ganzen habe ich Vertrauen in die Menschheit.	.815	.702
V_28 Ich bin der Meinung, dass Menschen generell zuverlässig sind.	.759	.629
V_29 Im Allgemeinen vertraue ich anderen Menschen, ausser es gibt Gründe, dies nicht zu tun.	.777	.627
		Cronbachs Alpha = 0.846

Vertrauen in die Institution (Institution based Trust)

Faktor 3	F-Ladung	Extraktion
V_20 Online-Anbieter behandeln ihre Kunden grundsätzlich anständig.	.613	.424

[58] Der Extraktionswert beim Item „Ich habe keine Bedenken, Online-Transaktionen durchzuführen." (V_16) war zu gering und wurde von der Faktorenanalyse ausgeschlossen. Der fünfte Faktor fällt weg, da nur zwei Items auf diesen Faktor bestätigt wurden: „Manchmal fühle ich mich unsicher, wenn ich im Internet meinen Interessen nachgehe." (V_17) und „Online-Anbieter übervorteilen normalerweise ihre Kunden nicht." (V_19). Ausserdem erwähnenswert ist die Zuteilung der beiden Items: „Ich finde es unproblematisch, dem gewählten Anbieter persönliche Daten zu überlassen." (V_64) und „Ich glaube, dass ich mich auf die Angebotsqualität des gewählten Anbieters verlassen kann." (V65). Diese wurden erstaunlicherweise dem Faktor „Vertrauen in den Online-Anbieter" (Faktor 1) zugerechnet, anstatt wie angedacht dem Faktor „Vertrauensabsicht" (Faktor 4).

V_21 Es gibt genug Sicherheitsmechanismen im Internet, damit ich es bedenkenlos für meine persönlichen Interessen nutzen kann.	.809	.680
V_22 Ich vertraue darauf, dass mich rechtliche Rahmenbedingungen vor Problemen im Internet bewahren.	.814	.700
V_23 Ich vertraue darauf, dass mich technische Anwendungen wie Verschlüsselungen vor Problemen im Internet bewahren.	.798	.671
V_24 Im Allgemeinen ist das Internet eine stabile und sichere Umgebung, um persönlichen Interessen nachzugehen.	.765	.630
		Cronbachs Alpha = 0.857

Vertrauensabsicht (Trusting Intensions)

Faktor 4	F-Ladung	Extraktion
V_61 Ich werde die Seite des gewählten Anbieters wahrscheinlich wieder besuchen.	.837	.818
V_62 Ich werde die Dienste des gewählten Anbieters in den nächsten drei Monaten erneut in Anspruch nehmen.	.884	.828
V_63 Ich würde die Seite des gewählten Anbieters anderen Personen weiterempfehlen.	.676	.702
		Cronbachs Alpha = 0.840

Unbenannter Faktor[59]

Faktor 5	F-Ladung	Extraktion
V_17 Manchmal fühle ich mich unsicher, wenn ich im Internet meinen Interessen nachgehe.	.751	.624
V_19 Online-Anbieter übervorteilen normalerweise ihre Kunden nicht.	.623	.568

Ausgeschlossene Items[60]

V_16 Ich habe keine Bedenken, Online-Transaktionen durchzuführen.

[59] Faktor 5 fällt weg, da nur zwei Items bestätigt wurden, für einen Faktor werden mindestens drei bestätigte Items benötigt.

[60] Dieses Item wurde von der Faktorenanalyse ausgeschlossen, da der Extraktionswert zu gering ist.

7.5 Auswertung der Vertrauenstypen (Forschungsfrage 1)

7.5.1 Mögliche zu verwendende Cluster-Algorithmen

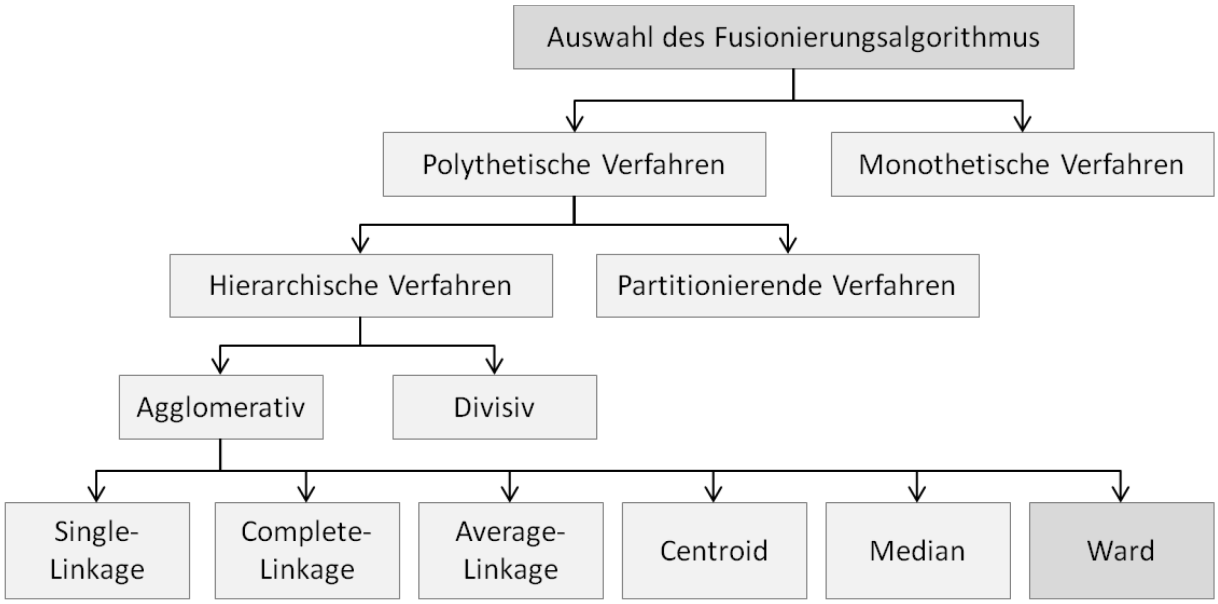


Abbildung 95: Überblick über mögliche Cluster-Algorithmen (eigene Darstellung in Anlehnung an Backhaus et al., 2011)

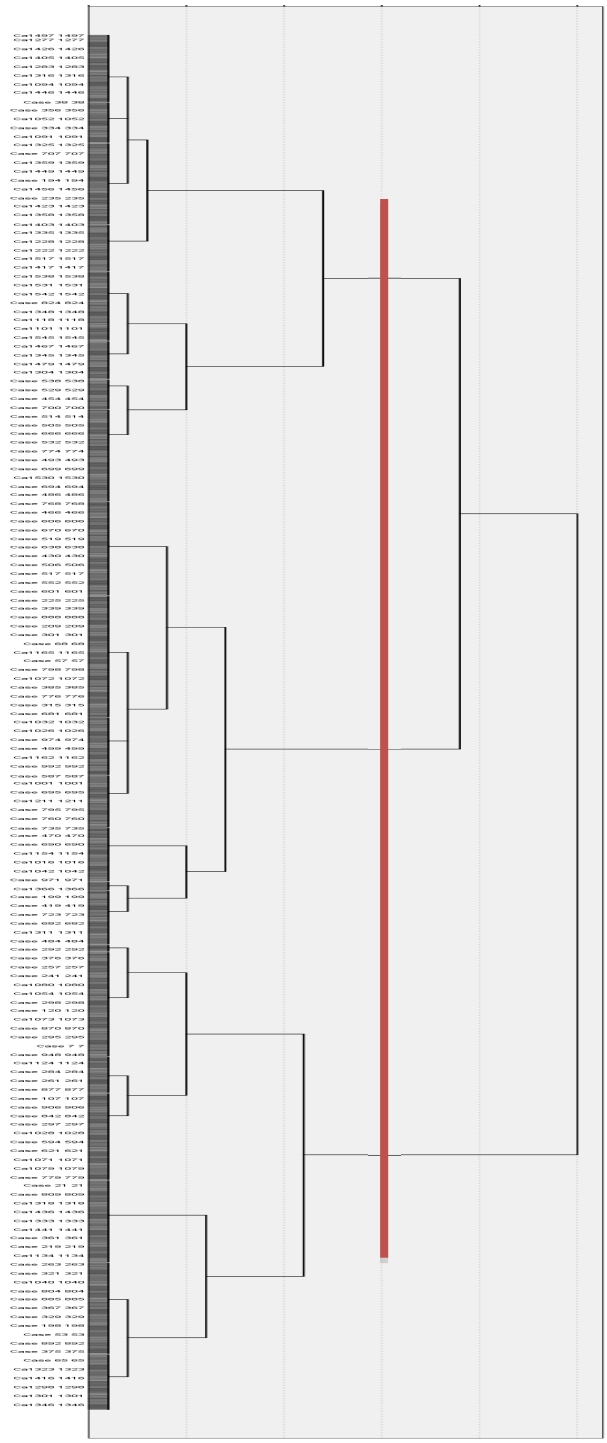
Werden alle Merkmalsvariablen zur Gruppierung der Objekte herangezogen, spricht man vom polythetischen Verfahren – im Gegensatz zum monothetischen Verfahren, bei dem immer nur jeweils eine Variable herangezogen wird, was äusserst selten der Fall ist. Beim polythetischen Verfahren kann wiederum zwischen partitionierenden (vorher festgelegte Anzahl Cluster) und hierarchischen Verfahren (Anzahl der Cluster ist unbekannt) unterschieden werden. Da die Anzahl der Cluster nicht vorherbestimmt ist, wird das hierarchische Verfahren angewandt, welches sich erneut zweiteilen lässt in einen agglomerativen (feinste Partition, Anzahl Cluster = Anzahl Objekte) und divisiven Algorithmus (gröbste Partition, alle Objekte befinden sich in einem Cluster). Das agglomerative Verfahren hat in der Praxis die grösste Bedeutung und ist unterteilt in das Single-Linkage-Verfahren (nächstgelegener Nachbar), das Complete-Linkage- (entferntester Nachbar), das Average-Linkage- (Linkage zwischen den Gruppen), das Centroid- (Abstände der Clustercentren), das Median- (Median der Cluster) und das Ward-Verfahren (Minimum-Varianz). Abbildung 95 liefert hierzu einen entsprechenden Überblick.

7.5.2 Zuordnungsübersicht anhand des Ward-Verfahrens (Ausschnitt)

Agglomeration Schedule

Schritt	Zusammengeführte Cluster		Koeffizienten	Erstes Vorkommen des Clusters		Nächster Schritt
	Cluster 1	Cluster 2		Cluster 1	Cluster 2	
1	1463	1497	.000	0	0	3
2	1426	1480	.000	0	0	4
…….						
…….						
…….						
1533	283	395	1181.338	1522	1481	1541
1534	2	90	1229.895	1529	1503	1538
1535	10	69	1278.606	1517	1528	1539
1536	6	8	1334.818	1513	1511	1542
1537	3	9	1395.634	1525	1496	1543
1538	2	277	1487.504	1534	1521	1546
1539	10	155	1593.379	1535	1520	1544
1540	17	340	1740.164	1532	1527	1544
1541	73	283	1893.913	1531	1533	1546
1542	1	6	2058.703	1530	1536	1545
1543	3	21	2241.943	1537	1524	1545
1544	10	17	2457.285	1539	1540	1547
1545	1	3	2802.321	1542	1543	1548
1546	2	73	3180.612	1538	1541	1547
1547	2	10	3808.297	1546	1544	1548
1548	1	2	4644.000	1545	1547	0

7.5.3 Dendrogramm des Ward-Verfahrens



7.5.4 Vertrauen in den Anbieter pro Vertrauenstyp in Prozent

Wohlwollend (V_56)

	Typ 1	Typ 2	Typ 3
trifft zu	2.9	54.2	32.7
trifft eher zu	25.4	33.1	46.3
neutral	61.1	12.2	17.2
trifft eher nicht zu	8.8	.2	1.2
trifft nicht zu	1.9	.0	.2
keine Antwort	.0	.4	2.4
Total	100	100	100

Kompetent (V_57)

	Typ 1	Typ 2	Typ 3
trifft zu	4.8	65.6	43.5
trifft eher zu	37.8	31.2	47.5
neutral	51.1	2.3	6.6
trifft eher nicht zu	5.2	.0	.2
trifft nicht zu	1.1	.0	.0
keine Antwort	.0	1.0	2.2
Total	100	100	100

Ehrlich (V_58)

	Typ 1	Typ 2	Typ 3
trifft zu	2.1	60.8	35.1
trifft eher zu	22.3	33.5	45.5
neutral	58.6	4.2	16.2
trifft eher nicht zu	13.4	.2	.4
trifft nicht zu	3.6	.0	.2
keine Antwort	.0	1.3	2.6
Total	100	100	100

Zuverlässig (V_59)

	Typ 1	Typ 2	Typ 3
trifft zu	4.0	67.3	41.3
trifft eher zu	30.2	30.0	46.3
neutral	53.6	1.7	8.8
trifft eher nicht zu	9.2	.2	1.0
trifft nicht zu	2.9	.0	.0
keine Antwort	0.2	.8	2.6
Total	100	100	100

Vertrauenswürdig (V_60)

	Typ 1	Typ 2	Typ 3
trifft zu	2.3	64.6	37.5
trifft eher zu	24.4	30.8	46.3
neutral	53.1	3.2	11.8
trifft eher nicht zu	13.7	.2	.8
trifft nicht zu	6.1	.0	.6
keine Antwort	.4	.2	3.0
Total	100	100	100

Sympathisch (V_176)

	Typ 1	Typ 2	Typ 3
trifft zu	3.6	57.4	36.1
trifft eher zu	29.6	30.2	41.5
neutral	55.5	11.0	18.0
trifft eher nicht zu	8.4	.0	.8
trifft nicht zu	2.3	.0	.4
keine Antwort	.6	1.3	3.2
Total	100	100	100

Ich finde es unproblematisch, dem gewählten Anbieter persönliche Daten zu überlassen. (V_64)

	Typ 1	Typ 2	Typ 3
trifft zu	7.1	49.8	27.3
trifft eher zu	21.2	27.9	36.7
neutral	43.3	17.1	22.6
trifft eher nicht zu	18.5	3.4	9.4
trifft nicht zu	9.7	.6	1.6
keine Antwort	.2	1.1	2.4
Total	100	100	100

Ich glaube, dass ich mich auf die Angebotsqualität des gewählten Anbieters verlassen kann. (V_65)

	Typ 1	Typ 2	Typ 3
trifft zu	7.6	62.4	41.7
trifft eher zu	33.8	29.8	42.3
neutral	45.6	5.9	12.6
trifft eher nicht zu	8.8	.2	.6
trifft nicht zu	3.8	.2	.0
keine Antwort	.4	1.5	2.8
Total	100	100	100

7.5.5 Vertrauensneigung pro Vertrauenstyp in Prozent

Im Allgemeinen habe ich Vertrauen zu anderen Menschen. (V_25)

	Typ 1	Typ 2	Typ 3
trifft zu	11.8	16.0	15.6
trifft eher zu	41.6	34.8	62.7
neutral	33.4	35.0	18.8
trifft eher nicht zu	10.3	12.2	2.0
trifft nicht zu	2.7	1.7	.8
keine Antwort	.2	.4	.0
Total	100	100	100

Ich verlasse mich meistens auf andere Menschen. (V_26)

	Typ 1	Typ 2	Typ 3
trifft zu	3.4	4.8	2.8
trifft eher zu	22.5	16.9	30.3
neutral	37.4	31.0	42.7
trifft eher nicht zu	27.5	34.4	20.4
trifft nicht zu	9.0	12.5	3.2
keine Antwort	.2	.4	.6
Total	100	100	100

Im Grossen und Ganzen habe ich Vertrauen in die Menschheit. (V_27)

	Typ 1	Typ 2	Typ 3
trifft zu	5.5	9.3	6.4
trifft eher zu	30.2	26.0	47.7
neutral	37.2	39.5	35.7
trifft eher nicht zu	21.8	18.6	8.6
trifft nicht zu	5.2	6.1	1.2
keine Antwort	.2	.4	.4
Total	100	100	100

Ich bin der Meinung, dass Menschen generell zuverlässig sind. (V_28)

	Typ 1	Typ 2	Typ 3
trifft zu	2.5	6.3	1.6
trifft eher zu	20.0	17.5	28.1
neutral	42.6	41.3	49.5
trifft eher nicht zu	26.1	26.4	17.4
trifft nicht zu	7.8	8.2	2.6
keine Antwort	1.0	.4	.8
Total	100	100	100

Im Allg. vertraue ich anderen Menschen, ausser es gibt Gründe, dies nicht zu tun. (V_29)

	Typ 1	Typ 2	Typ 3
trifft zu	12.8	15.2	19.8
trifft eher zu	38.4	34.2	53.9
neutral	31.1	35.2	21.6
trifft eher nicht zu	13.5	11.6	2.8
trifft nicht zu	3.6	3.4	.8
keine Antwort	.6	.4	1.0
Total	100	100	100

7.5.6 Vertrauen in die Institution pro Vertrauenstyp in Prozent

Online-Anbieter behandeln ihre Kunden grundsätzlich anständig. (V_20)

	Typ 1	Typ 2	Typ 3
trifft zu	3.2	11.8	1.0
trifft eher zu	19.8	34.6	14.4
neutral	51.9	43.2	56.3
trifft eher nicht zu	17.0	7.4	20.2
trifft nicht zu	6.9	.8	7.2
keine Antwort	1.1	2.3	.8
Total	100	100	100

Es gibt genug Sicherheitsmechanismen im Internet, damit ich es bedenkenlos für meine persönlichen Interessen nutzen kann. (V_21)

	Typ 1	Typ 2	Typ 3
trifft zu	4.2	14.3	.6
trifft eher zu	27.7	46.0	11.8
neutral	38.9	25.3	43.5
trifft eher nicht zu	21.9	11.8	32.3
trifft nicht zu	7.1	.8	11.6
keine Antwort	.2	1.9	.2
Total	100	100	100

Ich vertraue darauf, dass mich rechtliche Rahmenbedingungen vor Problemen im Internet bewahren. (V_22)

	Typ 1	Typ 2	Typ 3
trifft zu	4.6	14.1	10.6
trifft eher zu	29.4	42.0	35.1
neutral	32.4	27.0	37.3
trifft eher nicht zu	25.0	13.7	16.6
trifft nicht zu	8.4	2.1	.0
keine Antwort	.2	1.1	.4
Total	100	100	100

Ich vertraue darauf, dass mich technische Anwendungen wie Verschlüsselungen vor Problemen im Internet bewahren. (V_23)

	Typ 1	Typ 2	Typ 3
trifft zu	8.0	19.2	28.1
trifft eher zu	35.7	52.3	37.7
neutral	32.8	22.4	23.2
trifft eher nicht zu	16.0	4.8	10.4
trifft nicht zu	6.9	.0	.0
keine Antwort	.6	1.3	.6
Total	100	100	100

Im Allgemeinen ist das Internet eine stabile und sichere Umgebung, um persönlichen Interessen nachzugehen. (V_24)

	Typ 1	Typ 2	Typ 3
trifft zu	5.9	18.4	.8
trifft eher zu	30.5	44.9	23.4
neutral	38.5	26.8	42.7
trifft eher nicht zu	17.4	7.6	24.6
trifft nicht zu	5.7	.6	8.2
keine Antwort	1.9	1.7	.2
Total	100	100	100

7.5.7 Demografie und Internetnutzung pro Vertrauenstyp in Prozent

Geschlecht (V_135)

	Typ 1	Typ 2	Typ 3
weiblich	47.1	49.8	50.1
männlich	50.6	46.6	46.7
keine Antwort	2.3	3.6	3.2
Total	100	100	100

Alter (V_136)

	Typ 1	Typ 2	Typ 3
bis 15	13.0	6.1	11.4
16–25	13.2	11.4	10.8
26–45	27.7	25.5	25.5
46–65	26.0	28.3	24.8
66+	14.9	22.1	22.0
keine Antwort	5.3	6.7	5.4
Total	100	100	100

Höchster Bildungsabschluss (V_139)

	Typ 1	Typ 2	Typ 3
Hauptschulabschluss	4.4	8.6	5.6
Realschulabschluss	13.5	20.5	16.4
Berufsschule	17.6	23.8	18.8
Abitur / Fachabitur	18.1	16.0	18.8
FH / Studium	28.4	20.5	25.9
Sonstige	2.3	.6	1.6
noch in Ausbildung	15.3	9.5	12.6
keine Antwort	.4	.6	.2
Total	100	100	100

Erwerbstätigkeit (V_137)

	Typ 1	Typ 2	Typ 3
Angestellt (Vollzeit / Teilzeit)	35.7	39.2	**39.5**
Selbstständig erwerbstätig	10.1	10.3	7.6
Arbeitssuchend	3.4	3.8	3.4
in Ausbildung / Lehre	13.5	9.7	12.8
in Rente	19.8	**26.6**	26.1
Hausfrau/-mann	5.3	4.2	3.4
keine Antwort	12.0	6.2	7.2
Total	100	100	100

Branchen (V_138)

	Typ 1	Typ 2	Typ 3
Landwirtschaft / Bergbau	.8	.2	.4
Automobil / Luftfahrt / Schifffahrt	3.8	3.4	3.6
Bauwesen / Infrastruktur	3.1	2.7	2.2
Beratung / Recht	1.0	1.3	2.4
Informations- & Kommunikationstechnologien / Elektronische Geräte	5.0	4.0	3.8
Energie / Umwelt / Recycling	.6	1.0	1.2
Finanzen / Versicherung / Immobilien	4.8	4.6	5.6
Gesundheits- & Sozialwesen	**7.6**	6.8	6.4
Gross- und Einzelhandel	5.0	6.1	4.6
Kommunikation / Medien	1.9	2.3	3.0
Maschinenbau	1.3	2.5	3.0
Medizin / Pharma / Chemie	2.9	3.0	4.2
Nahrungs- und Genussmittel	1.7	.8	1.4
Öffentlicher Dienst	7.8	**10.5**	**10.6**
Tourismus / Gastgewerbe / Kultur / Sport	2.1	2.9	1.8
Transport / Logistik	2.1	3.2	2.8
Sonstiges	38.5	35.4	31.1
keine Angabe	10.1	9.5	11.8
Total	100	100	100

Internetnutzung (V_1)

	Typ 1	Typ 2	Typ 3
jeden Tag	91.8	93.0	90.8
mehrmals pro Woche	7.6	5.7	8.6
seltener	.0	.0	.2
keine Antwort	.6	1.3	.4
Total	100	100	100

Internetnutzung in Jahren (V_2)

	Typ 1	Typ 2	Typ 3
< 1 Jahr	.0	.4	.2
seit 1 Jahr	.8	.4	.2
seit 2 Jahren	1.9	1.1	1.2
seit 3 Jahren	5.0	4.0	5.2
seit 4 Jahren	5.2	5.1	6.6
seit 5 Jahren	12.2	11.2	7.8
seit 6 Jahren	6.7	8.7	7.0
seit 7 Jahren	6.3	5.1	4.8
seit 8 Jahren	5.9	9.9	7.2
> 8 Jahren	54.2	**52.1**	58.7
keine Antwort	1.9	1.9	1.0
Total	100	100	100

Private oder berufliche Internetnutzung (V_3)

	Typ	Typ 2	Typ 3
ausschliesslich beruflich	.2	0	.2
überwiegend beruflich	1.9	1.0	.8
sowohl beruflich als auch privat	48.3	46.2	48.7
überwiegend privat	24.4	22.8	23.8
ausschliesslich privat	24.2	29.7	26.3
keine Antwort	1.0	.4	.2
Total	100	100	100

E-Mail-Nutzung (V_4)

	Typ 1	Typ 2	Typ 3
jeden Tag	81.9	82.3	78.4
mehrmals pro Woche	14.1	14.1	16.4
einmal pro Woche	2.1	1.9	2.0
1- bis 2-mal im Monat	.8	.6	1.0
seltener	.2	.2	.6
nie	.2	.0	.6
keine Antwort	.8	1.0	1.0
Total	100	100	100

Informationssuche (z. B. auf Google) (V_5)

	Typ 1	Typ 2	Typ 3
jeden Tag	53.8	57.4	51.3
mehrmals pro Woche	36.1	33.8	35.5
einmal pro Woche	5.3	3.6	4.8
1- bis 2-mal im Monat	1.9	2.5	3.6
seltener	1.0	1.3	1.8
nie	1.0	0	1.0
keine Antwort	1.0	1.3	2.0
Total	100	100	100

Nutzung von Online-Banking (V_6)

	Typ 1	Typ 2	Typ 3
jeden Tag	12.8	**22.2**	13.8
mehrmals pro Woche	29.2	**34.2**	29.5
einmal pro Woche	21.4	**16.2**	19.4
1- bis 2-mal im Monat	9.5	8.0	8.4
seltener	3.4	3.8	2.6
nie	21.6	14.1	23.4
keine Antwort	2.1	1.5	2.8
Total	100	100	100

Nutzung von sozialen Netzwerken/Online-Communitys (V_7)

	Typ 1	Typ 2	Typ 3
jeden Tag	**34.4**	26.8	27.1
mehrmals pro Woche	**18.1**	14.6	16.2
einmal pro Woche	9.7	8.4	7.4
1- bis 2-mal im Monat	4.8	7.2	7.6
seltener	9.7	**15.4**	13.6
nie	22.3	25.7	26.9
keine Antwort	1.0	1.9	1.2
Total	100	100	100

Nutzung von Online-Shopping (V_8)

	Typ 1	Typ 2	Typ 3
jeden Tag	4.0	6.5	2.0
mehrmals pro Woche	13.2	16.3	14.2
einmal pro Woche	16.4	20.2	21.2
1- bis 2-mal im Monat	38.9	40.1	40.5
seltener	**22.5**	13.5	17.4
nie	4.8	2.7	4.0
keine Antwort	.2	.8	.6
Total	100	100	100

Nutzung von Online-Zeitungen (V_1v6)

	Typ 1	Typ 2	Typ 3
jeden Tag	**18.1**	20.0	17.2
mehrmals pro Woche	**17.7**	15.6	15.0
einmal pro Woche	**12.2**	12.2	12.0
1- bis 2-mal im Monat	11.8	8.7	13.4
seltener	20.4	22.2	19.8
nie	**18.9**	19.2	21.6
keine Antwort	.8	2.1	.8
Total	100	100	100

Nutzung von Online-TV/-Radio (V_9)

	Typ 1	Typ 2	Typ 3
jeden Tag	6.9	**10.6**	6.8
mehrmals pro Woche	12.8	**13.1**	10.8
einmal pro Woche	10.9	**10.8**	12.2
1- bis 2-mal im Monat	12.4	9.5	13.0
seltener	21.2	24.5	26.5
nie	34.4	29.5	29.3
keine Antwort	1.5	1.9	1.4
Total	100	100	100

Nutzung von Online-Dating (V_10)

	Typ 1	Typ 2	Typ 3
jeden Tag	2.5	**3.2**	.8
mehrmals pro Woche	1.5	**2.9**	2.2
einmal pro Woche	2.9	**2.3**	1.6
1- bis 2-mal im Monat	4.2	4.8	4.4
seltener	12.0	14.6	13.8
nie	75.8	**70.9**	76.0
keine Antwort	1.1	1.3	1.2
Total	100	100	100

Nutzung von Blogs (V_11)

	Typ 1	Typ 2	Typ 3
jeden Tag	5.5	4.9	3.6
mehrmals pro Woche	5.3	6.3	5.2
einmal pro Woche	4.8	5.7	6.2
1- bis 2-mal im Monat	8.2	8.4	7.4
seltener	19.8	17.5	19.2
nie	55.0	54.9	57.3
keine Antwort	1.3	2.3	1.0
Total	100	100	100

Nutzung von Twitter (V_12)

	Typ 1	Typ 2	Typ 3
jeden Tag	3.1	**3.0**	**2.0**
mehrmals pro Woche	4.0	**3.8**	**2.6**
einmal pro Woche	2.5	**3.0**	**3.2**
1- bis 2-mal im Monat	4.4	5.3	3.6
seltener	11.6	11.4	10.6
nie	73.1	**70.9**	76.6
keine Antwort	1.3	2.5	1.4
Total	100	100	100

Nutzung von Online-Games (V_13)

	Typ 1	Typ 2	Typ 3
jeden Tag	12.8	**13.7**	9.0
mehrmals pro Woche	10.7	**12.4**	10.0
einmal pro Woche	7.4	**7.8**	8.2
1- bis 2-mal im Monat	11.5	7.6	11.0
seltener	17.2	16.2	15.4
nie	38.9	40.7	45.3
keine Antwort	1.5	1.7	1.0
Total	100	100	100

7.5.8 Internetkompetenzen pro Vertrauenstyp in Prozent

Ich kann mir relevante Informationen im Internet beschaffen. (V_32)

	Typ 1	Typ 2	Typ 3
trifft zu	50.6	69.0	57.1
trifft eher zu	34.9	25.9	35.5
neutral	12.4	4.6	6.2
trifft eher nicht zu	1.3	.0	.2
trifft nicht zu	.6	.0	.4
keine Antwort	.2	.6	.6
Total	100	100	100

Ich kann abschätzen, welche Informationen im Internet zuverlässig sind. (V_33)

	Typ 1	Typ 2	Typ 3
trifft zu	22.7	30.2	19.4
trifft eher zu	43.3	49.2	48.7
neutral	25.0	16.2	24.6
trifft eher nicht zu	7.1	3.4	6.6
trifft nicht zu	1.5	.2	.6
keine Antwort	.4	.8	.0
Total	100	100	100

Ich vertraue meiner Fähigkeit, die Qualität einer Website einzuschätzen. (V_34)

	Typ 1	Typ 2	Typ 3
trifft zu	21.0	30.4	22.0
trifft eher zu	42.6	45.6	42.5
neutral	28.4	18.8	27.5
trifft eher nicht zu	7.1	3.2	7.2
trifft nicht zu	.8	.8	.4
keine Antwort	.2	1.1	.4
Total	100	100	100

Ich bin in der Lage, ein Profil in einem sozialen Netzwerk anzulegen. (V_35)

	Typ 1	Typ 2	Typ 3
trifft zu	43.3	45.4	42.1
trifft eher zu	18.5	20.2	23.4
neutral	20.2	16.3	14.6
trifft eher nicht zu	10.3	9.7	9.8
trifft nicht zu	7.1	7.6	9.6
keine Antwort	.6	.8	.4
Total	100	100	100

Ich bin in der Lage, ein Video im Internet zu publizieren (z. B. auf YouTube). (V_37)

	Typ 1	Typ 2	Typ 3
trifft zu	30.7	31.9	29.5
trifft eher zu	19.3	18.8	19.0
neutral	23.7	16.5	22.8
trifft eher nicht zu	15.3	16.2	14.2
trifft nicht zu	10.7	16.3	14.2
keine Antwort	.4	.2	.2
Total	100	100	100

Ich bin in der Lage, Informationen auf einem Blog oder bei Twitter zu veröffentlichen. (V_38)

	Typ 1	Typ 2	Typ 3
trifft zu	28.2	29.7	27.7
trifft eher zu	16.2	19.8	22.0
neutral	29.2	16.2	19.2
trifft eher nicht zu	14.5	14.8	15.2
trifft nicht zu	11.1	19.2	15.2
keine Antwort	.8	.4	.6
Total	100	100	100

Ich kann meine Gedanken und Ideen im Internet mitteilen. (V_39)

	Typ 1	Typ 2	Typ 3
trifft zu	25.2	29.5	27.9
trifft eher zu	21.9	25.3	26.5
neutral	32.8	23.2	24.4
trifft eher nicht zu	11.6	10.1	11.6
trifft nicht zu	8.2	11.4	9.4
keine Antwort	.2	.6	.2
Total	100	100	100

Ich bin in der Lage, einen Beitrag auf Wikipedia zu erstellen oder zu ergänzen. (V_40)

	Typ 1	Typ 2	Typ 3
trifft zu	20.4	21.1	21.6
trifft eher zu	25.2	21.9	21.8
neutral	29.8	23.8	26.7
trifft eher nicht zu	13.7	15.4	15.8
trifft nicht zu	10.1	17.5	13.0
keine Antwort	.8	.4	1.0
Total	100	100	100

Ich interessiere mich für neue Entwicklungen im Internet. (V_43)

	Typ 1	Typ 2	Typ 3
trifft zu	24.0	34.0	27.5
trifft eher zu	34.9	33.7	36.5
neutral	30.5	20.9	26.1
trifft eher nicht zu	6.7	7.6	7.0
trifft nicht zu	2.9	2.7	2.8
keine Antwort	1.0	1.1	.2
Total	100	100	100

Ich probiere gerne neue Online-Plattformen und Applikationen aus. (V_44)

	Typ 1	Typ 2	Typ 3
trifft zu	13.2	17.9	14.0
trifft eher zu	22.5	22.4	19.6
neutral	33.4	29.7	34.9
trifft eher nicht zu	20.8	19.0	18.2
trifft nicht zu	9.9	10.5	12.4
keine Antwort	.2	.6	.8
Total	100	100	100

7.5.9 Gewähltes Online-Geschäftsmodells pro Vertrauenstyp in Prozent

Gewähltes Online-Geschäftsmodell (V_177)

	Typ 1	Typ 2	Typ 3
Online-Shopping (z. B. Amazon, eBay, Lufthansa)	31.1	54.2	50.3
Online-Banking (z. B. Comdirect, Postbank, PayPal)	13.2	18.6	15.2
Soziale Netzwerke / Online-Community (z. B. Facebook, Xing, Parship)	37.8	15.4	18.2
Online-Information (z. B. Google, Zeitungen, Blogs, E-Mail, YouTube)	15.6	10.5	14.4
keine Antwort	2.3	1.3	1.8
Total	100	100	100

Konkreter Online-Anbieter (V_178)

	Typ 1	Typ 2	Typ 3
Amazon	6.3	22.4	18.0
eBay	7.3	7.4	5.6
H&M	.4	1.0	.2
Lufthansa	.2	.8	.4
Bank of Scotland	.4	1.5	.2
Comdirect	1.7	.6	1.4
Commerzbank	.2	.8	.2
ING-DiBa	.2	.8	.6
Paypal	2.1	3.6	2.8
Postbank	.4	2.7	1.6
Sparkasse	.8	.6	1.4
Facebook	23.7	6.1	4.6
Schüler VZ / StudiVZ / MeinVZ / WkW	2.9	2.9	3.2
Jappi	.6	.6	.8
Xing	1.1	.4	.6
Google	3.8	1.9	3.2
Twitter	.6	.6	.2
Web.de	.4	.2	.8
YouTube	1.7	.6	1.2
weitere	17.4	32.2	35.7
keine Angabe	28.0	12.7	17.2
Total	100.0	100.0	100.0

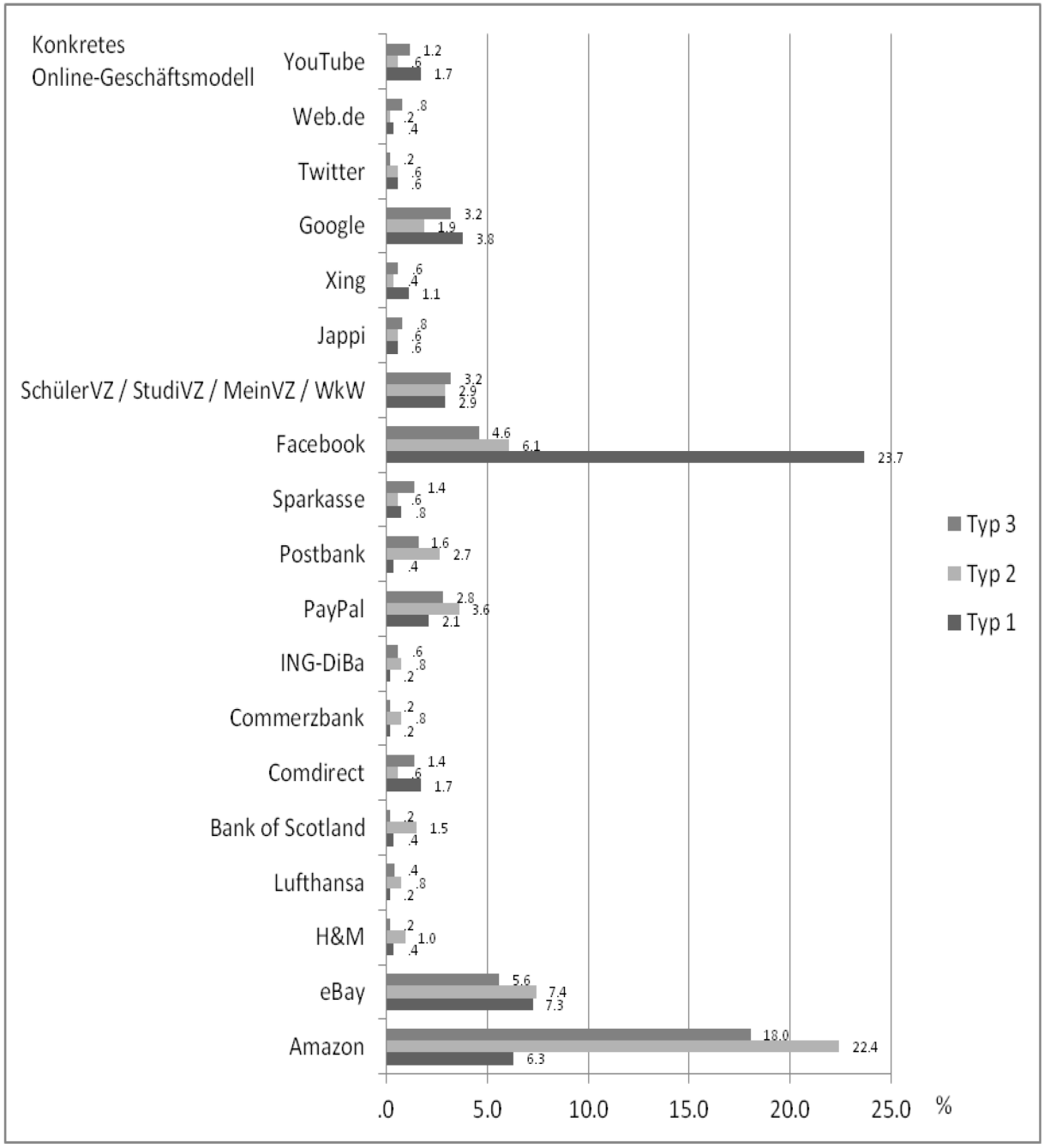


Abbildung 96: Typenunterscheidung anhand des konkreten Online-Anbieters in Prozent (V_178)

7.5.10 Typenunterscheidung anhand der „Keine Antwort“-Rate in Prozent

	Typ 1	Typ 2	Typ 3
Geschlecht (V_135)	2.3	3.6	3.2
Alter (V_136)	5.3	6.7	5.4
Höchster Bildungsabschluss (V_139)	0.4	0.6	0.2
Erwerbstätigkeit (V_137)	12	6.2	7.2
Branchen (V_138)	10.1	9.5	11.8
Internetnutzung (V_1)	0.6	1.3	0.4
Internetnutzung in Jahren (V_2)	1.9	1.9	1
Private oder berufliche Internetnutzung (V_3)	1	0.4	0.2
E-Mail-Nutzung (V_4)	0.8	1	1
Informationssuche (z. B. auf Google) (V_5)	1	1.3	2
Nutzung von Online-Banking (V_6)	2.1	1.5	2.8
Nutzung von sozialen Netzwerken/Online-Communitys (V_7)	1	1.9	1.2
Nutzung von Online-Shopping (V_8)	0.2	0.8	0.6
Nutzung von Online-Zeitungen (V_1v6)	0.8	2.1	0.8
Nutzung von Online TV/-Radio (V_9)	1.5	1.9	1.4
Nutzung von Online-Dating (V_10)	1.1	1.3	1.2
Nutzung von Blogs (V_11)	1.3	2.3	1
Nutzung von Twitter (V_12)	1.3	2.5	1.4
Nutzung von Online-Games (V_13)	1.5	1.7	1

7.6 Auswertung der Vertrauenstypen anhand der Vertrauensfaktoren (Forschungsfrage 2)

7.6.1 Items der Vertrauensfaktoren anhand des Mittelwertes pro Vertrauenstyp

Reziprozität	Typ 1 (n=524) Mittelwert St. Abw.	Typ 2 (n=526) Mittelwert St. Abw.	Typ 3 (n=499) Mittelwert St. Abw.	∑ (n=1'549) Mittelwert St. Abw.
V_73 Die Datenschutzbestimmungen sind leicht verständlich.	2.73 .989	2.04 1.04	2.40 1.079	2.39 1.068
V_76 Die allgemeinen Geschäftsbedingungen sind einfach zu verstehen.	2.77 .984	2.06 1.077	2.40 1.064	2.41 1.082
V_72 Die Datenschutzbestimmungen sind leicht zu finden.	2.65 1.010	2.00 1.044	2.30 1.037	2.32 1.064
V_75 Die allgemeinen Geschäftsbedingungen sind leicht zu finden.	2.65 .992	1.97 1.036	2.23 1.011	2.29 1.051
V_74 Der Anbieter verfügt über strikte Datenschutzrichtlinien.	2.68 .977	1.97 .997	2.29 1.036	2.31 1.043
V_78 Es ist gut erkennbar, welche Rechte ich dem Anbieter gegenüber habe (z. B. Garantien, Rückgaberecht).	2.63 .966	1.88 .922	2.15 .984	2.22 1.066
V_68 Der Anbieter erklärt mir, warum er welche Daten von mir benötigt.	2.80 1.013	2.01 1.058	2.37 1.066	2.42 1.085
V_71 Der Anbieter zeigt nachvollziehbar auf, wie er meine Daten verwendet.	2.79 1.012	2.05 1.008	2.48 1.034	2.44 1.062
V_79 Der Anbieter bietet viele Informationen über das eigene Unternehmen.	2.89 0.982	2.24 1.037	2.47 1.047	2.54 1.057
V_67 Der Anbieter fragt nur Daten ab, die er benötigt, um seinen Dienst betreiben zu können.	2.58 .995	1.78 .891	2.13 .987	2.16 1.013
V_77 Es ist gut erkennbar, welche Verpflichtungen ich eingehe (z. B. Kosten).	2.25 .976	1.64 .788	1.84 .923	1.91 .934

Marke & Design	Typ 1 (n=524) Mittelwert St. Abw.	Typ 2 (n=526) Mittelwert St. Abw.	Typ 3 (n=499) Mittelwert St. Abw.	∑ (n=1'549) Mittelwert St. Abw.
V_94 Es handelt sich um einen bekannten Anbieter.	2.16 .972	1.55 .864	1.75 .889	1.82 .944
V_97 Der Anbieter hat bereits viele Kunden bzw. Nutzer.	2.22 1.002	1.72 .989	1.77 .946	1.91 1.005
V_96 Der Anbieter existiert schon eine Weile.	2.16 .980	1.59 .834	1.77 .898	1.84 .936
V_100 Die Seite des Anbieters ist einfach und übersichtlich gestaltet.	2.32 .927	1.60 .821	1.82 .873	1.91 .924
V_95 Der Anbieter ist führend in seinem Bereich.	2.38 .962	1.87 .967	2.08 1.010	2.11 1.001
V_98 Das Design des Anbieters wirkt seriös und professionell.	2.44 .949	1.73 .877	1.95 .944	2.04 .971
V_102 Die Nutzung des Dienstes funktioniert genau so, wie ich das von ähnli-	2.38 .953	1.74 .914	1.87 .863	2.00 .952

chen Diensten schon kenne.				
V_103 Ich fühle mich auf der Seite wohl.	2.39 .942	1.63 .815	1.89 .867	1.97 .931
V_101 Links sind gut kenntlich gemacht.	2.41 .971	1.84 .975	2.07 1.00	2.11 1.008

Nutzerkontrolle	Typ 1 (n=524) Mittelwert St. Abw.	Typ 2 (n=526) Mittelwert St. Abw.	Typ 3 (n=499) Mittelwert St. Abw.	∑ (n=1'549) Mittelwert St. Abw.
V_119 Der Anbieter informiert mich, wenn er meine Daten an Dritte weitergibt.	2.90 1.118	2.42 1.199	2.68 1.207	2.66 1.19
V_120 Der Anbieter fragt mich um meine Zustimmung, bevor er meine Daten an Dritte weitergibt.	2.72 1.102	2.25 1.177	2.56 1.215	2.50 1.180
V_122 Der Anbieter ermöglicht mir, selbst auszuwählen, an wen meine Daten weitergegeben werden.	2.84 1.066	2.48 1.212	2.74 1.212	2.68 1.174
V_117 Die Angabe von Daten über das notwendige Minimum hinaus ist freiwillig.	2.56 1.017	2.21 1.078	2.36 1.043	2.38 1.055
V_123 Der Anbieter teilt mir mit, auf welche Art er meine Daten auswertet/analysiert.	2.96 1.049	2.47 1.160	2.75 1.179	2.72 1.148
V_121 Der Anbieter verzichtet ausdrücklich auf die Weitergabe meiner Daten an Dritte.	2.74 1.123	2.20 1.127	2.42 1.156	2.45 1.156
V_118 Ich weiss, welche meiner Daten der Anbieter gesammelt/gespeichert hat.	2.69 1.004	2.16 1.070	2.31 1.136	2.39 1.093

Kundenservice	Typ 1 (n=524) Mittelwert St. Abw.	Typ 2 (n=526) Mittelwert St. Abw.	Typ 3 (n=499) Mittelwert St. Abw.	∑ (n=1'549) Mittelwert St. Abw.
V_180 Der Anbieter stellt unterschiedliche Möglichkeiten zur Kontaktaufnahme zur Verfügung (Telefonnummer, E-Mail, Adresse).	2.78 1.168	2.11 1.121	2.38 1.180	2.42 1.188
V_179 Der Kundenservice des Anbieters ist freundlich.	3.00 1.116	2.20 1.167	2.57 1.166	2.59 1.195
V_114 Der Kundendienst ist einfach erreichbar.	3.03 1.116	2.31 1.196	2.60 1.163	2.65 1.196
V_115 Der Anbieter reagiert schnell auf meine Fragen/Bestellungen.	2.83 1.095	2.02 1.055	2.26 1.096	2.37 1.135
V_109 Die Kontaktdaten des Anbieters sind einfach zu finden (z. B. Adresse, Telefonnummer).	2.85 1.152	2.11 1.103	2.33 1.103	2.43 1.162
V_116 Der Anbieter stellt unterschiedliche Zahlungsmethoden zur Verfügung.	2.81 1.190	2.04 1.186	2.36 1.209	2.40 1.235

7.6.2 Items des Faktors Reziprozität pro Vertrauenstyp in Prozent

Die Datenschutzbestimmungen sind leicht verständlich. (V_73)

	Typ 1	Typ 2	Typ 3
stark beachtet	10.1	32.9	17.2
beachtet	27.9	38.4	36.9
neutral	44.7	19.4	30.7
wenig beachtet	11.6	5.3	8.4
nicht beachtet	5.3	3.0	4.6
keine Antwort	.4	1.0	2.2
Total	100	100	100

Die allgemeinen Geschäftsbedingungen sind einfach zu verstehen. (V_76)

	Typ 1	Typ 2	Typ 3
stark beachtet	9.4	34.0	16.6
beachtet	27.3	35.9	37.9
neutral	45.0	19.0	30.9
wenig beachtet	12.4	6.1	8.0
nicht beachtet	5.7	3.8	4.6
keine Antwort	.2	1.1	2.0
Total	100	100	100

Die Datenschutzbestimmungen sind leicht zu finden. (V_72)

	Typ 1	Typ 2	Typ 3
stark beachtet	11.3	36.3	18.2
beachtet	31.7	36.7	41.5
neutral	39.9	16.9	26.7
wenig beachtet	11.6	6.1	8.0
nicht beachtet	4.8	3.0	3.4
keine Antwort	.8	1.0	2.2
Total	100	100	100

Die allgemeinen Geschäftsbedingungen sind leicht zu finden. (V_75)

	Typ 1	Typ 2	Typ 3
stark beachtet	10.9	36.9	20.0
beachtet	32.4	37.6	42.7
neutral	40.8	16.5	25.3
wenig beachtet	10.3	4.4	7.0
nicht beachtet	5.2	3.6	2.8
keine Antwort	.4	1.0	2.2
Total	100	100	100

Der Anbieter verfügt über strikte Datenschutzrichtlinien. (V_74)

	Typ 1	Typ 2	Typ 3
stark beachtet	12.8	35.4	19.2
beachtet	26.3	39.4	40.1
neutral	45.8	16.5	27.9
wenig beachtet	10.7	5.3	7.2
nicht beachtet	4.4	2.5	3.4
keine Antwort	0.0	1	2.2
Total	100	100	100

Es ist gut erkennbar, welche Rechte ich dem Anbieter gegenüber habe (z. B. Garantien, Rückgaberecht). (V_78)

	Typ 1	Typ 2	Typ 3
stark beachtet	12.0	37.1	23.8
beachtet	30.7	40.7	42.5
neutral	42.4	16.2	24.2
wenig beachtet	10.9	3.2	5.0
nicht beachtet	3.8	1.7	2.6
keine Antwort	.2	1.1	1.8
Total	100	100	100

Der Anbieter erklärt mir, warum er welche Daten von mir benötigt. (V_68)

	Typ 1	Typ 2	Typ 3
stark beachtet	9.7	32.5	16.8
beachtet	26.1	36.5	40.7
neutral	43.3	20.0	26.7
wenig beachtet	14.5	7.0	9.6
nicht beachtet	5.9	3.2	4.0
keine Antwort	.4	.8	2.2
Total	100	100	100

Der Anbieter zeigt nachvollziehbar auf, wie er meine Daten verwendet. (V_71)

	Typ 1	Typ 2	Typ 3
stark beachtet	11.1	31.9	13.4
beachtet	23.9	34.6	38.1
neutral	45.2	23.6	33.5
wenig beachtet	13.9	6.7	8.8
nicht beachtet	5.7	1.3	4.6
keine Antwort	.2	1.9	1.6
Total	100	100	100

Der Anbieter bietet viele Informationen über das eigene Unternehmen. (V_79)

	Typ 1	Typ 2	Typ 3
stark beachtet	7.8	24.1	14.2
beachtet	21.6	40.7	35.7
neutral	49.6	23.6	33.3
wenig beachtet	13.7	7.2	11.2
nicht beachtet	6.9	3.8	3.4
keine Antwort	.4	.6	2.2
Total	100	100	100

Der Anbieter fragt nur Daten ab, die er benötigt, um seinen Dienst betreiben zu können. (V_67)

	Typ 1	Typ 2	Typ 3
stark beachtet	13.9	43.0	24.0
beachtet	32.8	38.2	42.3
neutral	38.7	13.3	23.2
wenig beachtet	10.1	3.2	6.2
nicht beachtet	4.4	1.1	2.0
keine Antwort	0.0	1.1	2.2
Total	100	100	100

Es ist gut erkennbar, welche Verpflichtungen ich eingehe (z. B. Kosten). (V_77)

	Typ 1	Typ 2	Typ 3
stark beachtet	24.2	50.0	38.1
beachtet	35.3	35.9	40.5
neutral	33.0	11.0	15.0
wenig beachtet	4.2	1.7	2.6
nicht beachtet	2.9	.4	1.8
keine Antwort	.4	1.0	2.0
Total	100	100	100

7.6.3 Items des Faktors Marke und Design pro Vertrauenstyp in Prozent

Es handelt sich um einen bekannten Anbieter. (V_94)

	Typ 1	Typ 2	Typ 3
stark beachtet	26.7	57.8	42.5
beachtet	38.2	27.9	36.9
neutral	27.9	9.3	15.0
wenig beachtet	4.0	1.5	2.2
nicht beachtet	2.7	1.5	1.0
keine Antwort	.6	1.9	2.4
Total	100	100	100

Der Anbieter hat bereits viele Kunden bzw. Nutzer. (V_97)

	Typ 1	Typ 2	Typ 3
stark beachtet	26.7	51.7	43.1
beachtet	34.9	30.2	35.3
neutral	29.2	11.6	14.0
wenig beachtet	6.3	2.3	3.6
nicht beachtet	2.5	3.2	1.4
keine Antwort	.4	1.0	2.6
Total	100	100	100

Der Anbieter existiert schon eine Weile. (V_96)

	Typ 1	Typ 2	Typ 3
stark beachtet	26.1	54.9	40.9
beachtet	39.3	32.1	39.7
neutral	26.7	9.1	13.0
wenig beachtet	4.2	1.5	3.0
nicht beachtet	2.9	1.3	1.2
keine Antwort	.8	1.0	2.2
Total	100	100	100

Die Seite des Anbieters ist einfach und übersichtlich gestaltet. (V_100)

	Typ 1	Typ 2	Typ 3
stark beachtet	17.7	52.1	35.9
beachtet	40.3	35.2	43.5
neutral	33.8	8.9	15.0
wenig beachtet	5.2	1.1	2.0
nicht beachtet	2.3	1.3	1.2
keine Antwort	.8	1.3	2.4
Total	100	100	100

Der Anbieter ist führend in seinem Bereich. (V_95)

	Typ 1	Typ 2	Typ 3
stark beachtet	18.3	42.6	29.9
beachtet	34.5	33.7	34.9
neutral	38.4	17.7	26.9
wenig beachtet	5.2	3.4	4.0
nicht beachtet	3.1	2.1	2.4
keine Antwort	.6	.6	2.0
Total	100	100	100

Das Design des Anbieters wirkt seriös und professionell. (V_98)

	Typ 1	Typ 2	Typ 3
stark beachtet	16.0	46.0	32.3
beachtet	33.8	38.4	41.7
neutral	39.3	11.2	18.4
wenig beachtet	8.0	1.7	4.0
nicht beachtet	2.1	1.9	1.6
keine Antwort	.8	.8	2.0
Total	100	100	100

Die Nutzung des Dienstes funktioniert genau so, (…). (V_102)

	Typ 1	Typ 2	Typ 3
stark beachtet	16.0	46.0	32.3
beachtet	41.0	36.7	43.3
neutral	33.0	12.2	19.6
wenig beachtet	6.1	1.7	1.0
nicht beachtet	3.2	2.3	1.0
keine Antwort	.6	1.1	2.8
Total	100	100	100

Ich fühle mich auf der Seite wohl. (V_103)

	Typ 1	Typ 2	Typ 3
stark beachtet	17.2	51.0	32.9
beachtet	34.2	32.9	42.9
neutral	39.9	12.5	18.8
wenig beachtet	5.5	1.7	2.6
nicht beachtet	2.3	.4	.6
keine Antwort	1.0	1.5	2.2
Total	100	100	100

Links sind gut kenntlich gemacht. (V_101)

	Typ 1	Typ 2	Typ 3
stark beachtet	17.9	42.0	27.3
beachtet	34.5	34.6	41.9
neutral	38.2	16.5	21.8
wenig beachtet	5.5	3.0	3.8
nicht beachtet	3.4	2.3	3.0
keine Antwort	.4	1.5	2.2
Total	100	100	100

7.6.4 Items des Faktors Nutzerkontrolle pro Vertrauenstyp in Prozent

Der Anbieter informiert mich, wenn er meine Daten an Dritte weitergibt. (V_119)

	Typ 1	Typ 2	Typ 3
stark beachtet	9.5	25.5	15.2
beachtet	21.6	26.6	25.3
neutral	44.7	31.0	37.5
wenig beachtet	12.2	8.4	9.8
nicht beachtet	10.9	7.4	10.0
keine Antwort	1.1	1.1	2.2
Total	100	100	100

Der Anbieter fragt mich um meine Zustimmung, bevor er meine Daten an Dritte weitergibt. (V_120)

	Typ 1	Typ 2	Typ 3
stark beachtet	12.6	31.7	19.0
beachtet	26.1	26.8	27.3
neutral	41.8	28.5	34.3
wenig beachtet	10.3	5.3	8.0
nicht beachtet	8.0	6.5	9.4
keine Antwort	1.1	1.1	2.0
Total	100	100	100

Der Anbieter ermöglicht mir, selbst auszuwählen, an wen meine Daten weitergegeben werden. (V_122)

	Typ 1	Typ 2	Typ 3
stark beachtet	9.4	23.4	13.8
beachtet	24.0	25.9	23.0
neutral	46.2	33.5	40.3
wenig beachtet	10.3	7.2	9.4
nicht beachtet	9.4	8.7	11.0
keine Antwort	.8	1.3	2.4
Total	100	100	100

Die Angabe von Daten über das notwendige Minimum hinaus ist freiwillig. (V_117)

	Typ 1	Typ 2	Typ 3
stark beachtet	13.4	26.4	16.8
beachtet	30.0	37.1	37.7
neutral	44.1	25.9	33.7
wenig beachtet	5.9	4.4	4.8
nicht beachtet	5.3	5.1	4.8
keine Antwort	1.3	1.1	2.2
Total	100	100	100

Der Anbieter teilt mir mit, auf welche Art er meine Daten auswertet/analysiert. (V_123)

	Typ 1	Typ 2	Typ 3
stark beachtet	6.5	20.7	11.4
beachtet	19.5	30.6	25.5
neutral	51.0	31.7	40.5
wenig beachtet	11.5	8.4	9.6
nicht beachtet	10.3	7.2	10.6
keine Antwort	1.3	1.3	2.4
Total	100	100	100

Der Anbieter verzichtet ausdrücklich auf die Weitergabe meiner Daten an Dritte. (V_121)

	Typ 1	Typ 2	Typ 3
stark beachtet	13.7	31.6	20.6
beachtet	22.1	29.1	30.7
neutral	43.7	27.0	33.3
wenig beachtet	10.9	6.7	6.2
nicht beachtet	8.2	4.6	7.0
keine Antwort	1.3	1.1	2.2
Total	100	100	100

Ich weiss, welche meiner Daten der Anbieter gesammelt/gespeichert hat. (V_118)

	Typ 1	Typ 2	Typ 3
stark beachtet	10.1	29.5	22.6
beachtet	29.4	36.7	32.7
neutral	43.7	23.0	29.7
wenig beachtet	10.5	5.7	7.0
nicht beachtet	5.3	4.2	5.2
keine Antwort	1.0	1.0	2.8
Total	100	100	100

7.6.5 Items des Faktors Kundenservice pro Vertrauenstyp in Prozent

Der Anbieter stellt unterschiedliche Möglichkeiten zur Kontaktaufnahme zur Verfügung (Telefonnummer, E-Mail, Adresse). (V_180)

	Typ 1	Typ 2	Typ 3
stark beachtet	9.9	33.3	21.2
beachtet	28.4	34.4	33.9
neutral	39.5	21.5	28.5
wenig beachtet	8.4	4.0	6.4
nicht beachtet	11.8	5.7	7.6
keine Antwort	1.9	1.1	2.4
Total	100	100	100

Der Kundenservice des Anbieters ist freundlich. (V_179)

	Typ 1	Typ 2	Typ 3
stark beachtet	5.3	31.0	14.8
beachtet	22.3	29.7	32.1
neutral	46.2	26.6	34.9
wenig beachtet	10.9	4.6	7.0
nicht beachtet	13.5	6.3	9.0
keine Antwort	1.7	1.9	2.2
Total	100	100	100

Der Kundendienst ist einfach erreichbar. (V_114)

	Typ 1	Typ 2	Typ 3
stark beachtet	6.5	28.1	14.8
beachtet	21.2	29.8	30.1
neutral	43.7	26.6	34.5
wenig beachtet	14.3	6.8	10.6
nicht beachtet	13.2	7.2	7.8
keine Antwort	1.1	1.3	2.2
Total	100	100	100

Der Anbieter reagiert schnell auf meine Fragen/Bestellungen. (V_115)

	Typ 1	Typ 2	Typ 3
stark beachtet	7.1	34.8	22.6
beachtet	28.6	37.3	36.9
neutral	41.0	19.8	27.7
wenig beachtet	12.0	2.3	5.4
nicht beachtet	9.5	4.8	5.0
keine Antwort	1.7	1.1	2.4
Total	100	100	100

Die Kontaktdaten des Anbieters sind einfach zu finden (z. B. Adresse, Telefonnummer). (V_109)

	Typ 1	Typ 2	Typ 3
stark beachtet	8.4	32.5	19.8
beachtet	29.4	37.6	38.1
neutral	38.7	18.6	27.1
wenig beachtet	9.5	5.1	7.6
nicht beachtet	12.6	5.3	5.0
keine Antwort	1.3	.8	2.4
Total	100	100	100

Der Anbieter stellt unterschiedliche Zahlungsmethoden zur Verfügung. (V_116)

	Typ 1	Typ 2	Typ 3
stark beachtet	11.8	39.7	22.2
beachtet	25.4	30.2	36.1
neutral	41.2	17.9	25.1
wenig beachtet	6.9	4.0	5.4
nicht beachtet	13.4	6.8	9.0
keine Antwort	1.3	1.3	2.2
Total	100	100	100

7.7 Auswertung der Vertrauenstypen anhand des Faktors Vertrauensabsicht (Forschungsfrage 3)

7.7.1 Items des Faktors Vertrauensabsicht pro Vertrauenstyp in Prozent

Ich werde die Seite des gewählten Anbieters wahrscheinlich wieder besuchen. (V_61)

	Typ 1	Typ 2	Typ 3
trifft zu	50.4	83.8	70.9
trifft eher zu	29.8	12.4	22.6
neutral	16.6	2.3	3.6
trifft eher nicht zu	1.3	.6	.6
trifft nicht zu	1.7	.2	.4
keine Antwort	.2	.8	1.8
Total	100	100	100

Ich werde die Dienste des gewählten Anbieters in den nächsten drei Monaten erneut in Anspruch nehmen. (V_62)

	Typ 1	Typ 2	Typ 3
trifft zu	46.8	68.4	61.3
trifft eher zu	27.9	20.0	22.2
neutral	20.4	8.2	11.6
trifft eher nicht zu	2.3	2.3	1.6
trifft nicht zu	2.1	.4	1.0
keine Antwort	.6	.8	2.2
Total	100	100	100

Ich würde die Seite des gewählten Anbieters anderen Personen weiterempfehlen. (V_63)

	Typ 1	Typ 2	Typ 3
trifft zu	26.7	66.0	53.7
trifft eher zu	27.9	22.8	26.9
neutral	34.9	9.3	14.8
trifft eher nicht zu	5.7	.6	1.0
trifft nicht zu	4.4	.6	1.2
keine Antwort	.4	.8	2.4
Total	100	100	100

7.8 Lebenslauf

Persönliche Daten

Name:	Andrea von Kaenel
Geburtsdatum:	18. Juni 1980
Nationalität:	Schweizerin
Heimatorte:	Greifensee ZH & Reichenbach BE

Berufliche Tätigkeit

02/2009 – 08/2012	Research Assistant, Universität St.Gallen, St.Gallen, Institut für Medien- und Kommunikationsmanagement, 70 %
06/2010 – 08/2010	Research Assistant, Harvard University, Boston, USA, Internship am Berkman Center for Internet and Society
07/2004 – 10/2008	Studentische Mitarbeiterin, BMW Finanzdienstleistungen (Schweiz) AG, Dielsdorf
03/2002 – 09/2003	Trademark Assistant Intellectual Property, ABB Schweiz AG, Baden

Bildung

02/2009 – 08/2013	Doktoratsstudium Betriebswirtschaftslehre, Schwerpunkt Marketing & Kommunikation, Institut für Medien und Kommunikationsmanagement, Universität St.Gallen
10/2006 – 01/2009	Master of Arts in Marketing, Dienstleistungs- und Kommunikationsmanagement, Universität St. Gallen
10/2003 – 08/2006	Betriebsökonomin FH, Fachhochschule Nordwestschweiz, Baden & Windisch, Vertiefungsrichtung Marketing
02/2002 – 10/2003	Kaufmännische Berufsmaturität, AKAD in Zürich
08/1997 – 08/2000	Kaufmännische Verwaltungslehre, Gemeindeverwaltung Obersiggenthal AG